

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Better Law-making and Evaluation for the EU Digital Rulebook

Bassini, Marco; Maggiolino, Mariateresa; De Streel, Alexandre

Published in:
Media laws

Publication date:
2025

Document Version
Publisher's PDF, also known as Version of record

[Link to publication](#)

Citation for pulished version (HARVARD):

Bassini, M, Maggiolino, M & De Streel, A 2025, 'Better Law-making and Evaluation for the EU Digital Rulebook', *Media laws*, no. 2, pp. 177-223.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Better Law-making and Evaluation for the EU Digital Rulebook*

Marco Bassini, Mariateresa Maggiolino,
Alexandre de Streel

Table of Contents

1. Introduction. – 2. Methodology: Our Approach to Analysing the EU Digital Rulebook. – 3. In-Depth Analysis: Unpacking the EU Digital Rulebook. – 4. *Ex-post* Evaluations. – 5. Policy Recommendations

1. Introduction

In recent years, the European Union (EU) has proactively developed a comprehensive regulatory framework aimed at governing the digital economy and addressing the profound economic and social transformations brought about by the rise of digital technologies and the datafication of reality. This framework, often referred to as the “EU digital rulebook”, consists of key legislative acts such as the General Data Protection Regulation (GDPR),¹ the Data Governance Act (DGA),² the Data Act (DA),³ the Platform-to-Business Regulation (P2BR),⁴ the Digital Services

* This paper builds upon the report “*Better Law-Making and Evaluation for the EU Digital Rulebook*,” published by the Centre on Regulation in Europe (CERRE), available at cerre.eu. Marco Bassini authored Sections 1, 3.1, and 3.4; Mariateresa Maggiolino authored Sections 2, 3.2, and 3.3; Alexandre de Streel wrote Section 4; Section 5 is the result of the authors’ joint efforts.

L’articolo è stato sottoposto, in conformità al regolamento della Rivista, a referaggio “a doppio cieco”.

¹ 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, and repealing Directive 95/46 (General Data Protection Regulation), OJ [2016] L 199/1.

² Regulation 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation 2018/1724 (Data Governance Act), OJ [2022] L 152/1.

³ Regulation 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation 2017/2394 and Directive 2020/1828 (Data Act) OJ L 2023/2854, 22.12.2023.

⁴ Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services, OJ [2019] L 186/55.

Act (DSA),⁵ the Digital Markets Act (DMA),⁶ and the recent Artificial Intelligence Act (AI Act).⁷ Furthermore, other pieces of legislation driven by the digital transformation include the REFIT of the Audiovisual Media Services Directive (AVMSD),⁸ the Digital Single Market Copyright Directive,⁹ and the European Code of Electronic Communications.¹⁰ Equally important are the legislative stances concerning cybersecurity, such as the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive),¹¹ the European Cyber Resilience Act (CRA),¹² the Digital Operational Resilience Act (DORA), as well as the European Media Freedom Act (EMFA),¹³ and the Regulation on the Transparency and Targeting of Political Advertising.

EU digital rulebook therefore consists of a set of laws that were meant to have a structural impact on the so-called digital ecosystem. Not by coincidence, a significant part of these laws came into being following pre-existing attempts to regulate the respective subject matters, such as in the case of the GDPR (which repealed and replaced the Data Protection Directive) and the DSA (which replaced the E-Commerce Directive). Instead, the DMA came into force as a sort of *lex specialis*, which was necessitated by the unprecedentedly disruptive nature of the developments

⁵ Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31, OJ [2022] L 277/1.

⁶ Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828 (Digital Markets Act), OJ [2022] L 265/1.

⁷ Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations 300/2008, 167/2013, 168/2013, 2018/858, 2018/1139 and 2019/2144 and Directives 2014/90, 2016/797 and 2020/1828 (Artificial Intelligence Act), OJ L, 2024/1689.

⁸ 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 audio-visual media services (Audiovisual Media Services Directive), OJ [2010] L 95/1, as amended by Directive 2018/1808.

⁹ Directive 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9 and 2001/29, OJ [2019] L 130/92.

¹⁰ 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.

¹¹ Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation 910/2014 and Directive 2018/1972, and repealing Directive 2016/1148 (NIS 2 Directive), OJ [2022] L 333/80.

¹² Regulation 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations 168/2013 and 2019/1020 and Directive 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024.

¹³ Regulation 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13 (European Media Freedom Act), OJ L, 2024/1083, 17.4.2024.

in data and digital markets, for which the EU treaty provisions were no longer suitable.

From a purely formal perspective, these developments reflect a growing recognition that the mere harmonisation of Member States' laws is no longer sufficient to effectively address the far-reaching consequences of the digital transformation that has unfolded over the past decade. On the substantive side, various factors have clearly triggered and shaped the relevant legislative initiatives. Foremost among these is the protection of fundamental rights, which has emerged as one of the most frequently cited drivers of recent developments in the EU digital rulebook—either on its own or in conjunction with other objectives, such as ensuring fairness and equity among economic agents and social actors.¹⁴

Equally significant is the harmonisation of the internal market, which has consistently served as a cornerstone and legal basis for many of the laws comprising the EU digital acquis. Furthermore, it should not be overlooked that the promotion of innovation, job creation, and economic growth has frequently been highlighted as a central economic objective of these new Regulations and Directives.¹⁵

Combining all these value-driven and economic goals is even more difficult where relevant reforms, in addition to their legal added value, are also a consequence of political bargaining. The global battle for so-called digital sovereignty has inspired many of the legislative reforms that came into being in the last decade: the AI Act stands out as evidence of EU institutions' interest in “moving first” and hoping to derive the benefits associated with this strategy. Politically, the goal of digital sovereignty also appears in the EU institutions' desire to promote a “Brussels effect” specifically through digital policy, which is a comparatively favourable arena for establishing *de facto* influence. Safeguarding fundamental rights in the face of an unprecedented succession of technological developments has been a key argument used by EU lawmakers to justify regulatory intervention. As an example, this justification came into play in the approval of the GDPR and, more recently, of the AI Act, in light of the crucial value attached to the fundamental right to data protection, amongst others.

And if what has been said were not enough, it must be noted that European institutions have endeavoured—or are now striving—to shape and interpret these Regulations and Directives with an aim to minimise regulatory costs. In doing so, they seek to avoid burdening businesses, thereby preserving their drive to remain competitive and innovative.¹⁶

¹⁴ Regulations that fall in the scope of the EU digital rulebook are therefore multifaceted, aiming both to align regulation with the goal of a high level of protection of the EU's flagship rights, such as data protection and to foster harmonisation in the internal market in strategic domains. As such, the two objectives are not in conflict with each other, although it might not always be easy to fulfil them both equally.

¹⁵ That said, the EU institutions may well have conceived these rules independently of their economic impact, guided instead by broader considerations of governance and policy coherence.

¹⁶ *Speech by President von der Leyen at the European Parliament Plenary on the new College of Commissioners and its programme*, in *neighbourhood-enlargement.ec.europa.eu*, 27 November 2024, which reads: «[f]or Europe to catch up, we will also need to make things easier for our companies. They are telling us that the regulatory burden weighs heavily on them. Too

Another growing priority in EU policymaking is proofing legislation against security risks, including - but not limited to - the digital sphere, as stated in the European Commission's 2024-2029 Political Guidelines, which sets out the objective of integrating 'security-by-design' into EU policymaking. These observations unveil the existence of larger political drivers behind the most important EU digital rulebook reforms in the past decade.

That said, the question this report aims to address is whether the various approaches adopted by EU institutions were consistent with the legal justifications given for the adoption of the laws that shaped the EU digital rulebook. In order to address this question, this report will delve into the specific tool of impact assessments to understand how EU lawmakers took the Better Regulation principles into account while evaluating the existing market failures and the solutions to be adopted. This analysis will be conducted with respect to a selection of laws that had a significant impact on data and digital services, the impact of which can now be assessed in greater detail compared to other more recent pieces of legislation.

Understanding the shortcomings of impact assessments for the acts falling within the EU digital rulebook is a key objective in light of the unprecedented developments in technology that occurred over the past decade, the commitment to improving simplification, streamlining regulation and improving legal certainty, and the need for more future-proof legislation. In order to properly develop an *ex post* impact assessment and call for possible improvements in the EU digital rulebook, it is therefore imperative to explore "what worked and what did not work" in the making of the various legal acts, i.e., to look specifically at their assessment of existing market failures and the design of the legislative responses. This analysis is carried out bearing in mind that impact assessments are generally conducted at the beginning of the legislative process, and so the "failures" (or "successes") of the EU digital rulebook may also depend on the changes and amendments made by the co-legislators (i.e., the Council and Parliament) at a later stage. However, we believe that stronger and more thorough impact assessments at the very early stages of the legislative process can pave the way for legislation that is more resistant to political bargaining.

2. Methodology: Our Approach to Analysing the EU Digital Rulebook

Broadly speaking, the expression "Better Regulation" (BR) refers to a policy approach and framework aimed at improving the quality, efficiency, and effectiveness of laws and regulations. The concept is particularly significant within the EU, where it has evolved over several decades,

much reporting. Too many overlaps. And too complex and costly to comply with. We need to streamline our rules to reduce the burden on businesses. And we need to give legal certainty about what we expect from them».

beginning to influence policy discourse as early as the 1990s,¹⁷ resulting in the publication of several official documents.¹⁸

The impetus for advocating for robust BR at the EU level has been driven by several compelling reasons. Primarily, there is a pressing need to decrease the volume of regulations and associated regulatory costs while simultaneously improving the quality of laws and policies formulated within the EU.¹⁹

Moreover, these years have been marked by growing scepticism among EU citizens and businesses, often fuelled by perceptions of excessive bureaucratic burdens and concerns about decision-making processes that seem increasingly distant from the citizens of Member States. Therefore, BR serves a dual purpose: it elucidates the development of EU institutions and technical structures while also offering a means to better understand the Union's approach to governance, particularly in relation to internal policy improvement and the reduction of red tape. In this way, BR helps to nurture public trust in the EU's regulatory framework.²⁰

Finally, by ensuring that decision-making occurs at the most appropriate level, thereby safeguarding the sovereignty of Member States, BR is seen as a necessary measure to uphold the principle of subsidiarity and counter the phenomenon of "competence creep", wherein the EU gradually acquires more power from sovereign Member States in legislative and decision-making processes.²¹

Therefore, today BR is a key part of efforts to streamline regulatory processes and ensure that legislation fulfils the following (main) objectives:

- *Reducing Unnecessary Regulatory Burdens*: BR aims to minimise costs and administrative burdens by cutting down on redundant or overly complex regulation (red tape) that slows down investments and hinder businesses, citizens, and public authorities;
- *Enhancing the Quality of Legislation*: BR intends to create well-designed, coherent laws based on thorough impact assessments. Legislation must be fit for purpose, remain relevant over time, and align with long-term policy objectives, such as sustainability and digital readiness;
- *Ensuring Proportionality and Subsidiarity*: Laws should be proportionate

¹⁷ C. Dunlop – C.M. Radaelli, *Policy learning in the European Union*, in P.R. Graziano - J. Tosun (eds.), *Elgar encyclopedia of European Union public policy*, Cheltenham-Northampton, 2022, 612.

¹⁸ European Commission, *Better Regulation: taking stock and sustaining our commitment*, COM(2019)178 final; European Commission, Commission Staff Working Document, *Better Regulation Guidelines*, Brussels, 3.11.2021, SWD(2021) 305 final. To be sure, these documents do not establish any binding rules. Specifically, the Guidelines and the Toolbox serve as internal instructions as well as practical and hands-on instruments for the Commission's staff.

¹⁹ U. Pachl, *Repercussions of the European Commission's Better Regulation Agenda on Consumer Interests and Policy*, in *European Journal of Risk Regulation*, 6(3), 2015, 375; F. Simonelli – N. Iacob, *Can We Better the European Union Better Regulation Agenda?*, in *European Journal of Risk Regulation*, 12(4), 2021, 849.

²⁰ S. Garben, *A taste of its own medicine: Assessing the impact of the EU Better Regulation Agenda*, in *European Law Journal*, 26(1-2), 2020, 83.

²¹ C. Foster, *Research Agendas for the Digital Economy*, in *Sociology*, 54(5), 2020, 1041.

to the issues they address and respect the principle of subsidiarity, ensuring decisions are made at the most appropriate level of governance, whether local, national, or EU-wide;

- *Improving Transparency and Accountability:* The legislative process should be open to public scrutiny, with clear documentation and explanation of the evidence and rationale behind regulatory actions. This enhances the legitimacy and accountability of EU decisions;
- *Fostering Competitiveness and Innovation:* By reducing regulatory complexity and focusing on essential, high-quality legislation, Better Regulation creates a favourable environment for economic growth, competitiveness, and innovation; and
- *Adopting an Overall Coherent Approach:* All EU legislation should align with high-level and long-term policy goals, such as the European Climate Law, digital transformation, and the United Nations Sustainable Development Goals (SDGs). Strategic foresight is essential to ensure that policies are future-proof.

In summary, BR is not about deregulation or reducing the scope of government intervention but rather about making regulation smarter and more effective. To realise these goals, BR must rely on:

- *A True Participative Approach:* All stakeholders, including businesses, consumers, experts, individuals, and groups affected by EU laws, should be able to contribute to policy- and rule-making by expressing their views and providing relevant data;
- *Evidence- and Experience-Based Rules:* BR must be informed by the best available evidence, ranging from quantitative data such as statistics and measurements to quality data, such as stakeholders' opinions and academic evaluations, ensuring that laws are grounded in reliable and up-to-date information. Furthermore, policy- and rule-makers should continuously improve legislation by learning from the implementation and application of EU rules. The "evaluate first" principle should guide the revision of existing laws to adapt to changing circumstances and the EU's diverse needs;
- *Future-proof rules:* BR must be made of rules that are designed to remain effective, relevant, and adaptable over time, even as societal, technological, economic, and environmental conditions evolve. Indeed, the world is constantly changing, and regulatory frameworks need to be resilient and flexible enough to address emerging challenges and opportunities without becoming outdated or requiring frequent, substantial revisions. This is why BR must consider long-term trends and potential scenarios; must allow for adjustments as circumstances change; and must be crafted to encourage innovation rather than stifle it, by being open to new technologies and business models; and
- *The One-in, One-out Principle,* under which every new piece of legislation concluded by the EU requires the repeal of an existing one, reflects a response to one of the main criticisms of the EU legislative process: the excessive bureaucratic burdens, over-

regulation, and the rising costs associated with implementation, execution, and compliance.²² However, it is important to note that there may be certain policy areas where an increase in legislation, rather than a reduction, is necessary.

Since 2001, EU institutions have made significant efforts to shape their law-making processes in line with the BR principles.²³ They have streamlined procedures, outlined them in well-structured handbooks, and enhanced digital tools supporting public consultations, such as the portals where Calls for Evidence are available and the Fit for Future platform.

Today, this approach has become standard practice, embraced by EU institutions when drafting digital laws. That is why we have decided to put this method to the test, focusing on three key pieces of current EU digital rulebook: the GDPR, the DSA, and the DMA. We are looking at the GDPR because, since it came into effect in 2018, we have started to gather empirical data that shows whether the Commission's impact predictions were on target. As for the DSA and DMA, both are set to produce significant changes in the functioning of digital markets, and we want to dig deeper into the empirical evidence the Commission used to justify such major regulatory moves.

In this report, to carry out these tasks, we focus on analysing the Commission's *ex ante* impact assessments, which were issued before the final drafts of the relevant laws were prepared. Policymakers and regulators use impact assessments as tools for accountability, reporting on the law-making process. Specifically, *ex ante* impact assessments document the evidence analysed, the goals pursued, and the options considered before enacting new rules. In *ex post* impact assessments, policymakers and regulators monitor the outcomes of adopted rules to determine if revisions are needed. Thus, in this report, we will analyse existing impact assessments to determine whether and how the European Commission (EC) applied the principles and methods of Better Regulation in developing the EU digital rulebook (a backwards-looking analysis). To be sure, changes may occur between the RIAs and the approval of the final laws. As a result, the law that comes into force may diverge from the evidence on which the Commission based its proposal. However, whether those changes are positive or negative, they are typically not backed by new assessment. Instead, they stem from political negotiations at the European Parliament and the Council, highlighting that the final legal rules are not entirely evidence-based by definition.

Additionally, we will discuss how future *ex post* evaluations should be

²² F. Simonelli – N. Iacob, *Can We Better the European Union Better Regulation Agenda*, cit.; C. Dunlop – C.M. Radaelli, *Policy learning in the European Union*, cit.; S. Garben, *Policy learning in the European Union*, cit.; C.M. Radaelli, *Whither better regulation for the Lisbon agenda?*, in *Journal of European Public Policy*, 14(2), 2007, 190.

²³ See European Commission, *Better Regulation*, in commission.europa.eu, where it is explained how EU institutions follow the principles of BR by ensuring law-making is transparent, evidence-based, and inclusive. This involves assessing the impacts of proposed laws, simplifying rules, and reducing burdens through initiatives like the REFIT programme. Public consultations are integrated into the process via the “Call for Evidence” and digital platforms, allowing stakeholders to provide input. Strategic foresight is also employed to develop policies that are future-proof and aligned with sustainability goals.

conducted, offering guidance to the EC on applying Better Regulation principles and methods when revising the EU digital rulebook (a forward-looking analysis).

3. In-Depth Analysis: Unpacking the EU Digital Rulebook

This section presents an analysis of the *ex ante* impact assessments that preceded the adoption of the GDPR, DSA, and DMA. Each sub-section follows the same structure: after briefly introducing each law and its goals, it delves into the impact assessments, specifically highlighting issues that were not fully considered in the assessment.

3.1. GDPR's *Ex Ante* Impact Assessment: Weaknesses and Missed Opportunities

The GDPR is one of the first and one of the most prominent pieces of the EU digital rulebook. Although the GDPR is a technology-neutral law, it was adopted to increase the level of protection of personal data, and then of individuals, in light of the large-scale advent of digital technologies. It is not coincidental that various “battles” for digital sovereignty, especially concerning the US-EU relationship, deal with the extraterritorial application of EU data protection law and, in particular, the GDPR.²⁴ In such a vein, the GDPR is also the legal act that exemplifies the interest of the EU to act as “first-movers” and so take advantage of the so-called “Brussels effect”.²⁵

Indeed, the pre-existing legal framework, consisting of the implementation of Directive 95/46/EC by Member States, could not capture the magnitude of the consequences of the digitisation process that occurred in the two decades following the entry into force of the Data Protection Directive. This is also why, in the absence of future-proof legislation, it was up to the Court of Justice of the European Union (CJEU) to provide some practical solutions by way of interpreting EU law in light of the technological developments.²⁶

²⁴ See the ECJ judgments in Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (2015) and Case C-311/18 *Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems* (2020).

²⁵ A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford, 2020.

²⁶ See for instance the *Google Spain* judgment, Case C-131/12, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, (2014), and the *Schrems I and II* judgments, cit., issued in 2014 and 2015 respectively. Also, in 2014 the Court of Justice invalidated the Data Retention Directive (in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*) finding it in contrast with arts. 7, 8 and 52 of the Charter of Fundamental Rights of the European Union. These stances are very telling of the approach of the Court of Justice (and similarly of the EU legislator) vis-à-vis data protection, which commentators have described as «Europe's First Amendment» (see B. Petkova, *Privacy as Europe's first Amendment*, in *European Law*

The market failures that the GDPR aims to tackle mostly deal with imbalances deriving from power and information asymmetries between data controllers and individuals in their capacity as data subjects. These imbalances are largely rooted in the profound transformations in the economic and social sphere, known as the digital transformation, which also resulted in the rise of big tech companies largely relying on large datasets.

One of the main goals of the GDPR, then, lies in empowering individuals and strengthening their control over the use of personal information in the context of multi-party, cross-border, and digitalised processing activities in a more and more data-driven economy.

The GDPR pursues this goal by establishing legal mechanisms that operationalise the accountability principle, which is binding for data controllers and amounts to the main pillar of the regulation. The GDPR also tackles possible externalities that are consequential to the inherent power imbalances between data controllers and data subjects, by requiring the proactive implementation of risk-measured solutions that are instrumental, e.g., to reduce the likelihood of data breaches and other possible violations, and thus to increase individuals trust (also in their capacity as consumers in the data-driven economy). In this respect, the GDPR aims to remove these externalities (which are inherent in processing activities and cannot be entirely removed or prevented) by creating additional costs in terms of compliance for data controllers, which increasingly value compliance with data protection regulation as a reputational factor. The GDPR also established mechanisms that make its provisions applicable to non-EU based controllers, thereby avoiding any possible risk of circumvention, most notably by companies that have their business based in the US – including, but not limited to, big tech companies. As recent developments illustrate,²⁷ compliance with data protection law also has key value in avoiding anticompetitive conduct, by preventing or reducing possible data oligopolies or monopolies. Ultimately, another goal behind the GDPR was to eliminate the inherent costs (in terms of negative externalities) deriving from a fragmented legal framework consisting of 27 different pieces of legislation applicable in the EU which could significantly diverge in their content.

The GDPR faced these challenges by articulating a legal framework modelled on a risk-based approach, consistent with the key role played by the principle of accountability.²⁸ By adhering to the risk-based approach (which also is the blueprint of the more recent AI Act, despite the existence of significant divergences between the two approaches²⁹), the

Journal, 25(2), 2019, 140.

²⁷ See among others the judgment of the Court (Grand Chamber) in Case C-252/21, *Meta Platforms Inc and Others v. Bundeskartellamt* (2023).

²⁸ See R. Gellert, *The Risk-Based Approach to Data Protection*, Oxford, 2020; K. Demetrou, *GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved*, in E. Kosta – J. Pierson – D. Slamanig – S. Fischerhübner – S. Kren (eds.), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Berlin, 2018, 137.

²⁹ In the GDPR the risk-based approach requires controllers to comply with heightened obligations and to properly implement the data protection by design and by default

regulation leaves room to differentiate the compliance depending on the risk scenario and makes it (and the relevant costs) adaptive to the specific circumstances and processing activities. Furthermore, the principle of accountability further contributed to empowering individuals vis-à-vis data controllers that process their personal data. The internalisation of the costs for data protection violations was carried out by establishing severe penalties in case of failure to comply with the applicable provisions under the GDPR. However, this is also one of the elements that trigger some thoughts on the adequacy of this framework: should companies and public agencies comply “because” of the risk of incurring serious penalties? Or should compliance with data protection law rather constitute a key value in a broader perspective? This alternative also describes the line between actual and effective compliance and merely formal compliance.

3.1.1. Goals and Benefits of the GDPR

The impact assessment accompanying the proposal of the EC for a regulation released in 2012 pointed out three problems in EU data protection law.

The first problem consisted of the existence of barriers for organisations and public authorities, depending essentially on three different but intertwined factors: fragmentation, legal uncertainty, and inconsistent enforcement. Fragmentation was mostly caused by the existence of the (then) 28 different pieces of legislation that granted Member States significant room in the implementation of Directive 95/46/EC. While the ability of Member States to transpose EU law could pave the way for accommodating national specificities, and overall ensure greater flexibility, this factor contributed to increased uncertainty at the same time. All the more, this held true in light of the resulting inconsistencies in the enforcement of data protection law by the respective supervisory authorities, which were formally interpreting and applying different pieces of legislation. The combination of these factors constituted a source of costs and administrative burdens for organisations that had to navigate a complex landscape with differing requirements in each Member State, ultimately also resulting in an increased risk of non-compliance and incurring penalties. Particularly, the existence of varying approaches across Member States could result in discrepancies between the very same practices and ultimately suggest, under certain circumstances, an increase in forum shopping. Such a scenario *de facto* undermined the free flow of personal data that the same Directive 95/46/EC aimed to secure. This first problem can be described as related to an internal market dimension. The second problem identified in the impact assessment concerned the lack of individuals’ control over their personal data. This problem deals with the fundamental rights dimension inherent in data protection.

principles by adopting risk-measures responses, while in the AI Act the risk-based approach mostly reflects in the categorisation of AI systems according to risk clusters and, consequently, in the imposition of specific requirements and obligations for providers and deployers.

The obsolescence of Directive 95/46 became quickly visible as soon as digitisation extended to most of the economic, social, and legal relationships. As noted above, the GDPR is a technology-neutral piece of legislation; however, it would be largely inappropriate to consider it technology-agnostic, as the fundamental rights dimension of personal data came into play most notably as a consequence of the shift to a data-driven economy and society and thus focusing on the data-driven providers. Additionally, the very same reasons behind the first problem outlined above, i.e., fragmentation, legal uncertainty, and inconsistent enforcement, equally affected individuals in their capacity as data subjects.

The third problem mentioned by the impact assessment related to a specific domain within EU data protection where inconsistencies and gaps were particularly evident and problematic, namely that of police and judicial cooperation in criminal matters. As is well known, the specific response to this problem came in the form of the Law Enforcement Directive (Directive 2016/680).

The main drivers of these problems were, therefore, Member States' diverging national laws (resulting in unnecessary costs and administrative burdens) and the lack of trust by individuals depending on the perceived lack of or reduction in control over their personal data, for instance, because of the difficulties inherent in exercising their rights as data subjects. It is not by coincidence that in 2014 the Court of Justice's *Google Spain* judgment, delivered on the basis of Directive 95/46/CE but also "looking forward" to the then-anticipated GDPR, marked a significant development towards the protection of data subjects. Among other things, the Court made it clear that EU data protection law applies regardless of whether data controllers, who are subject to the relevant obligations, are established, to the extent they target European residents. This way, the Court brought to an end the frequently made argument that processing activities only occurred in non-EU countries and were therefore immune from the application of EU data protection law. The decision had a huge impact on the well-established interpretation of Directive 95/46 by courts and supervisory authorities, and ultimately on big tech companies, which could no longer object to the extraterritorial application of EU law.

In this transition, the EU lawmaker was supported by the Court of Justice in enhancing the fundamental rights dimension of personal data protection. However, the plan to revisit EU data protection law also consisted of other goals than the protection of fundamental rights, including ensuring the proper functioning of the internal market, enhancing coherence in the data protection framework and addressing specific market failures.

As a result, among the various policy options considered, the impact assessment conducted by the European Commission precisely suggested the adoption of a Regulation (in combination with other measures for the specific sector of police and judicial cooperation). A new Regulation, giving rise to an increase in the level of harmonisation, was seen as the most suitable form of intervention to pursue the goals and safeguard the values identified in the impact assessment.

As the existing literature illustrates, the coming of the GDPR has not been without costs and uncertainties for organisations operating in Member

States and, generally speaking, cross-border businesses. In articulating and addressing the main sources of criticism, this analysis acknowledges that the impact assessment was drafted on the basis of a specific proposal for a Regulation that later went through significant changes as a result of the legislative process, and whose enforcement and implementation turned out to be rather fragmented. We do not argue that the weaknesses and unintended consequences of the GDPR are only the result of an improper methodology in the framing of the impact assessment; our claim, though, is that impact assessments should generally resist the influence of political bargaining. A robust impact assessment, in other terms, should be sufficiently persuasive and methodologically grounded to preserve its role of “guidance” even as it is faced with the “perils” of the legislative process. At the same time, EU institutions should perhaps reconsider the role and value of impact assessments as an enduring component of the legislative process.

Prior to undertaking a comprehensive examination of potential enhancements to be evaluated in an *ex post* impact assessment, it is imperative to conduct a nuanced analysis of the consequences of the GDPR. This necessitates an objective assessment of the indisputable advantages and benefits that the regulation has brought about.

From a purely legal standpoint, the GDPR has established a framework that reduces legal uncertainty. While Member States retain the option of adopting more specific provisions in certain areas as outlined in the GDPR, it is unlikely that this will result in the emergence of new inconsistencies and discrepancies. The inconsistencies mainly result from fragmented implementation and enforcement. Member States and the respective supervisory authorities should therefore align to a common and unique enforcement framework and proper cooperation and consistency mechanisms are now established with a view to avoid diverging approaches. In theory, the establishment of the one-stop-shop mechanism reflects a deeper understanding of the business models of organisations engaged in cross-border processing activities and the inherent complexities in terms of enforcement, however in practice, its implementation has been complex.

The GDPR undoubtedly reduced the gaps and asymmetries between individuals (data subjects) and organisations (data controllers), by re-balancing this relationship and empowering data subjects in more visible terms. It can be said that the coming of the new legal framework incentivised trust by consumers and created more awareness both by individuals with respect to their personal data and by organisations and public authorities with regard to their obligations. As noted, compliance with data protection law has now acquired a reputation value, given the huge impact on individuals, their privacy and other fundamental rights related to the processing of personal data. There is a new business culture and the principle of accountability at the heart of the GDPR definitely contributed to increasing the level of attention and investments in compliance.

3.1.2. The Costs of the GDPR

These are undisputed advantages that emerged after the GDPR's entry into force. Organisations and individuals, in their respective roles as controllers and data subjects, can feel and appreciate these advantages, acknowledging them as the added value of the GDPR. However, these benefits did not come without costs. Some of these costs were estimated in the impact assessment, while others were not or were just partially estimated. In fact, the impact assessment also developed a framework to estimate the consequences of a chosen policy option on competitiveness. However, some of the assumptions about the actual impact of the GDPR seem to have been misplaced, as confirmed recently by the Draghi Report on European competitiveness.³⁰ In our view, there are at least three components of costs to be considered.

3.1.3. Compliance Costs

The first category of costs includes compliance costs. An in-depth analysis of the compliance issues raised by the GDPR and its interpretation by courts and supervisory authorities falls outside the scope of this report. However, we focus on the cost analysis developed in the impact assessment as far as compliance is concerned, in order to highlight how the assessment failed to consider possible additional costs deriving from the overall impact of the new legal framework.

The impact assessment addressed the economic and financial impacts of the policy options 1 and 2 together. The analysis of the estimated costs concerned two measures in particular, the obligation to designate a data protection officer (DPO) and the obligation to conduct data protection impact assessments, both applicable under certain circumstances.

As far as the *designation of DPOs* is concerned, the impact assessment underlined that “the obligation for larger economic operators only (more than 250 employees) to designate DPOs is not expected to create disproportionate costs, as DPOs are already common in large and multinational companies whose business is linked with the processing of personal data”.³¹ The impact assessments estimated compliance costs to amount to € 320 million per annum for large companies in total but highlighted that these costs could be reduced in the scenario whereby groups of companies would appoint a single DPO for the group. Also, the assessment pointed out that “SMEs would be excluded from this obligation,

³⁰ M. Draghi, *The future of European competitiveness*, September 2024.

³¹ Commission Staff Working Paper, Impact Assessment, *Accompanying the document* Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, 69 (hereinafter, also “GDPR & LED Impact Assessment”).

except if their core activity consists of processing operations which require regular and systematic monitoring”.³² The assessment, particularly in Annex 6, ventured into a detailed analysis, which nevertheless largely relied on assumptions. For instance, the impact assessment assumed that 90% of large enterprises (i.e., with more than 250 employees) had already staff performing comparable duties so that just 10% of the relevant share (i.e., 4,000 out of 40,000 large enterprises) would face an actual cost for designating a DPO. Considering that the cost for employing a full-time DPO was estimated at € 80,000 per annum, the total labour cost was calculated at € 320 million per annum.

Regarding the conduct *Data Protection Impact Assessments (DPIAs)*, the impact assessment made clear that this requirement would apply only on a case-by-case basis depending on the specific risk scenarios. The document also detailed the estimated costs for small-scale DPIAs, medium-scale DPIAs and large-scale DPIAs,³³ outlining the benefits for businesses in identifying and managing major data protection risks and thus improving the security of data.³⁴ Curiously enough, the document noted that “the reporting costs of a DPIAs would be the least costly part of a DPIA – the real costs will be in determining whether a DPIA should be conducted, gathering information about the project, deciding whether to engage stakeholders [...], identifying the risks and only then preparing a DPIA report, making recommendations, following up on those recommendations to ensure they are actually implemented”.³⁵

As ancillary requirements, the impact assessment also found the obligation to have records of the processing activities and to operationalise the data protection by design and by default principle not to create significant economic impacts.

A few years after the entry into force of the GDPR, the impact assessment seems to have largely underestimated the compliance costs implied by the new law.

First of all, these costs cannot be simply limited to the costs incurred for designating DPOs and conducting DPIAs. The advent of the GDPR determined a profound change in the paradigm of data protection and compliance with this new scheme, centred on the principle of accountability, which required significant efforts, also in terms of costs. Apparently, the impact assessment does not pay any regard to this “Copernican revolution”, failing to capture the actual consequences on data controllers.

A second critical point concerns the underestimation of the actual economic and financial impact of the GDPR, most notably on the scope of application. The assessment was perhaps too optimistic in estimating the number of controllers impacted by the new obligations, failing to foresee that the reputational value of compliance with data protection law

³² *Ibid.*

³³ GDPR & LED Impact Assessment, 70; amounting, respectively, to € 14,000, 34,500 and 149,000. See also Annex 6, 122 ff.

³⁴ *Ibid.*, 70.

³⁵ *Ibid.*, 122.

would have fostered many SMEs (small and medium-sized enterprises) and controllers to undertake some requirements only to increase the trust of consumers and better align to their competitors. It also failed to estimate the impact of compliance costs depending, among others, on activities such as handling requests to exercise data subjects' rights, liaising with data protection authorities and structuring proper procedures (including for data transfers or data breach notifications or communications). It is telling that the designation of DPOs has become a best practice adopted even by controllers who are not bound to do so by the GDPR. According to an IAPP 2019 study, approximately 500,000 organisations registered DPOs across the EU under the GDPR.³⁶ The study could not estimate how many of the subjects that registered a DPO were public authorities or private sector organisations. However, it is evident that the actual number of designations in 2019 significantly exceeded the estimated number of required DPOs indicated in the impact assessment. The spread of awareness and emergence of a “data protection culture”, alongside appropriate practices, has to be seen as one of advantages of the GDPR and is thus welcome as a positive development. However, these advantages did not come without a cost, and the impact assessment does not seem to consider the inherent complexity of compliance costs. In fact, the impact assessment was based on the assumption that enterprises could simply internalise the costs associated with the designation of DPOs by reallocating tasks currently performed by individuals in other roles. At the same time, even DPIAs acquired a growing importance and soon became a key requirement in the context of GDPR compliance, due to the unprecedented technological developments that occurred in the last decade. Many of the processes that have been affected by the digital transformation involve the processing of personal data. The implementation of innovative technological solutions ranks among the criteria pointed out by the Article 29 Working Party in its guidelines, as an index of processing activities “likely to result in high risks”.³⁷ Accordingly, while proving to be key for ensuring data security, DPIAs became more and more common and far from a requirement applicable only to the most sophisticated (and “risky”) processes and actors.

The fact that the actual compliance costs outnumbered those estimated in the impact assessment also depends on the fact that the GDPR is formally a technology-neutral regulation, which nonetheless became key in a variety of respects (e.g., for governing the first applications of AI technologies, such as in the context of automated-decision making) in such peculiar transition. This means that the efforts and attention that public authorities and especially enterprises had to devote to GDPR compliance were perhaps higher than expected also because of the critical role of this piece of legislation.

³⁶ IAAP, *Study: An estimated 500K organizations have registered DPOs across Europe*, in *iapp.org*, 16 May 2019.

³⁷ Article 29 Data Protection Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation 2016/679*, 17/EN, WP 248, 4 April 2017, 8.

3.1.4. Effects on Competition and Reduced Contestability

The second category of costs that the impact assessment has failed to properly take into account is the negative effects on competition and the reduced contestability. As noted in law and economics literature, in practice, the GDPR does not foster competition and reflects a limited understanding of data-based markets.³⁸ Accordingly, the regulation may have met its ambition of positively impacting the fundamental rights dimension of data protection but appears to have enhanced to a limited extent only the internal market dimension.

To strengthen the protection of individuals' personal data, the EU lawmakers introduced more severe restrictions on the ability to collect and use personal data by controllers.³⁹ The empowerment of data subjects resulted in new constraints for data controllers wishing to gather personal information as part of their everyday business. This had all the more of a significant impact against the background of a data-driven society where emerging technologies (such as AI) largely rest upon the availability of vast amounts of data for both their development and deployment, as the most recent developments highlight very well.⁴⁰ Of course, the fact that some market actors managed to collect large amounts of datasets in the context of the digital economy does not necessarily imply that they will benefit from a competitive advantage in the AI market, given the availability of other key resources, such as synthetic data and non-personal data, for the development of AI models and systems.

However, the adoption of a risk-based approach did not necessarily implicate higher compliance costs for the largest controllers. Indeed, the fact that the largest organisations were found to already comply with some of the requirements introduced by the GDPR (as was the case with DPO designation), had the effect of reducing the overall compliance costs to be incurred, due to the already applied corresponding national legislative requirements. In addition, compliance costs had a proportionally more limited impact on the largest organisations, while more significantly affecting other market players.

The fact that the overall impact of compliance costs could not by definition parallel the size of the entities acting as controllers and that the specific weight of compliance costs was, therefore, higher for smaller and medium businesses, made the existence of some effects on competition apparent.

³⁸ See among others D. Geradin – T. Karanikioti – D. Katsifis, *GDPR Myopia: how a well-intended regulation ended up favouring large online platforms – the case of ad tech*, in *European Competition Journal*, 17(1), 2020, 47; M. Gal – O. Aviv, *The competitive effects of the GDPR*, in *Journal of Competition Law & Economics*, 16(3), 2020, 349.

³⁹ See G. Aridor – Y. Che – T. Salz, *The effect of privacy regulation on the data industry: empirical evidence from GDPR*, in *The RAND Journal of Economics*, 54(4), 2023, 695, , which for example focus on advertising services to highlight how the coming of the GDPR resulted in smaller firms, generally dependant on third party access, suffering from reduced ability to collect data and then conduct business because of users' opting out.

⁴⁰ See Italian Data Protection Authority, *ChatGPT, the Italian data protection authority closes the preliminary investigation. OpenAI will have to carry out a six-month information campaign and pay a fine of EUR 15 million*, 21 December 2024, doc. no. 10085432.

In other terms, compliance turned out to be relatively more costly for smaller and medium organisations than for the largest organisations. Moreover, similar effects on competition are due to the limitations derived from the GDPR in terms of availability of data and constraints for their collection. In a data-driven economy some organisations, particularly those operating in the digital ecosystem, managed to gather large datasets because of the nature of their business models. Scholars have pointed out that the impact of the restrictions imposed by the GDPR were more limited for these companies, often big digital platforms. In other terms, collecting data became more difficult for every market player, but organisations that need to gather large datasets suffered the impact of the GDPR restrictions more than others.⁴¹

Geradin and others have described these effects as «GDPR's unintended consequences».⁴² They observe that, although the right to data portability bears a remarkable potential to foster competition in digital markets, the GDPR may overall increase market concentration. This conclusion is rooted in a variety of reasons.

A first reason lies in the compliance costs, which in the authors' view may cause not only barriers to entry but also incentives for some players to exit. This finding is consistent with the empirical evidence regarding some players that had a presence – albeit virtual – in the EU that opted for not targeting European residents anymore in order to escape the application of the GDPR as a result of a cost-benefit analysis.⁴³ Such an exit strategy was chosen in all the circumstances where compliance with the GDPR was considered simply not affordable. This remark is consistent with the finding that compliance costs turned out to be proportionally higher for smaller organisations, while easier to absorb for larger companies. This risk of market players “leaving” the EU is not factored into the impact assessment, which has not paid sufficient regard to the magnitude of the consequences of the extraterritorial application of the regulation, notably in light of the diverging understanding of privacy and data protection in other jurisdictions, such as the US, where they do not enjoy a comprehensive legal framework at the federal level. This factor could be considered as a possible externality generated by the GDPR compliance costs.

As a second reason, the authors maintain that large platforms benefit from consumers' trust. In their view, the fact that large platforms can easily internalise compliance costs and view compliance as an unavoidable step, given the strict monitoring by supervisory authorities and the risk of incurring severe penalties, ultimately results in a more favourable

⁴¹ In a similar vein, see also G.A. Johnson – S. K. Shriver – S.G. Goldberg, *Privacy & market concentration: Intended & unintended consequences of the GDPR*, in *Management Science*, 69(10), 2023, 5695.

⁴² D. Geradin – T. Karanikioti – D. Katsifis, *GDPR Myopia*, cit., 62.

⁴³ For an overview of the overall impact of the coming into force of the GDPR from this perspective, see also C. Peukert – S. Bechtold – M. Batikas – T. Kretschmer, *Regulatory Spillovers and Data Governance: Evidence from the GDPR*, in *Marketing Science*, 41(4), 2022, 746; G.A. Johnson – S. K. Shriver – S.G. Goldberg, *Privacy & market concentration*, cit.; G. Presidente – C. B. Frey, *The GDPR effect: How Data Privacy Regulation shaped firm performance globally*, CEPR, 10 March 2022.

perception by consumers.⁴⁴ Consumers' increased trust may also depend on the feeling that some market players are more and/or better regulated than others, bringing to light a possible advantage of asymmetric regulation. In addition, platforms having leading positions in the relevant markets⁴⁵ can more easily obtain users' consent.⁴⁶ Less directly, it is argued that the one-stop-shop mechanism, while providing more clarity and legal certainty, ultimately results in benefitting companies located in friendly jurisdictions. However, this effect may be relatively weak as we see in practice that the one-stop-shop mechanism is not always applied rigorously.

However, the key factor that various commentators have pointed out as a source of negative effects on competition lies in the restrictions the GDPR brings along on data collection and data sharing. Gal and Aviv observed that such limitations could «prevent the emergence of better data-based products or services» and «reduce firms' ability to develop and fine-tune new algorithms, which might increase productive and dynamic efficiency in a wide array of markets».⁴⁷ This looks precisely at the intersection between the dynamics that the GDPR aimed to govern (the lack of proper control in a data-driven economy fostered by the digital transformation) and the developments that may have occurred just a few years later and that have now become more visible. While the lawmakers' concern for individuals and the lack of proper control over their data (which resulted in the efforts to strengthen the fundamental rights dimension of data protection) is understandable, the impact of these unintended consequences may in turn reduce the advantages of digitisation for individuals and the society at large. So, the digital transformation process may not deliver its promises in the end.

Furthermore, Gal and Aviv found that the effects of these limitations may take different shapes. For example, they maintain that the restrictions in question could prevent firms from obtaining the data necessary for their operations or at a minimum reduce their ability to collect such data. These barriers may result in additional costs for companies wishing to obtain external data or in the impossibility for them to obtain sufficient data to

⁴⁴ With respect to the value of trust, see Campbell et al., *supra*, according to which a setting may emerge where «large firms have no inherent advantage over small firms in generating trust».

⁴⁵ Other authors such as G.A. Johnson – S. K. Shriver – S.G. Goldberg, *Privacy & market concentration*, cit., highlight the existence of unintended consequences deriving from the GDPR and ultimately favouring large platforms. They notice, in particular, a short-run increase in aggregate concentration, depending on the non-mechanical nature of the trade-off between data minimisation (a key principle that the GDPR aims to foster in data processing) and market concentration. They also see a risk that personal data processing becomes in turn more concentrated as the increase in concentration concerns platforms such as web technology vendors having the ability to process data, thus calling for a balance between concentration of data ownership and increase of market power.

⁴⁶ See also C. Peukert – S. Bechtold – M. Batikas – T. Kretschmer, *Regulatory Spillovers and Data Governance*, cit., 764, where the authors note that the consent requirement for websites «disproportionately benefits larger firms offering a broader range of services», so that «the larger a service provider becomes, the cheaper it may become to gather broad user consent».

⁴⁷ M. Gal – O. Aviv, *The competitive effects of the GDPR*, cit., 382.

enjoy economies of scale and scope in data analysis.⁴⁸ The restrictions on the collection of data do not seem to be countered by the increase in the amount of data provided by individuals as a result of higher trust in data controllers and generally in GDPR-compliant processing of personal data.⁴⁹ Additionally, anticompetitive effects may take the form of more concentrated market structures. In the authors' view, this would be the result of two intertwined dynamics, namely higher comparative advantages for larger firms to meet the GDPR requirements and reduced emergence of competitive and distributed data collection ecosystems.⁵⁰

The adoption of the DMA a few years later may perhaps provide support to these findings. Even if the DMA aims to tackle problems that EU competition law could not address on the basis of its well-established tools, its adoption demonstrates that data markets were far from immune from problems such as market concentration and reduced contestability. Finally, Gal and Aviv highlight a critique that is deeply rooted in the GDPR impact assessment: the negative consequences on international competitiveness,⁵¹ a concern that they and other authors have consistently voiced, in particular regarding the advent of artificial intelligence technologies. One could argue that the subsequent adoption of the AI Act⁵² aims to remedy possible technological gaps that the EU suffers compared to other jurisdictions such as the US and China. Similar questions on the impact of the AI Act on international competitiveness are now being discussed among scholars, given the uncertain ability of this stance to give rise to a Brussels effect.⁵³

However, back to the GDPR, Gal and Aviv believe that the regulation, while properly tackling individuals' concerns for the protection of personal data as a fundamental right, has not sufficiently considered the key value of data sharing and synergies. The authors note that in its impact assessment the Commission concluded that the GDPR would have strengthened competition and supported the competitiveness of EU firms. However, the document "disregards important factors such as the effects of the GDPR on the ability of firms to enjoy data-based advantages by way of data synergies and economies of scale and scope in data analysis, which may significantly affect competition and innovation".⁵⁴

⁴⁸ *Ibid.*, 381.

⁴⁹ As noted by Gal and Aviv, *ibid.*, 382, some commentators found a possible counterargument in the possibility for individuals to feel a stronger sense of safety for their data by virtue of the protections provided by the GDPR, most notably in the information technology context: see A. Acquisti – C. Taylor – L. Wagman, *The Economics of Privacy*, in *Journal of Economic Literature*, 54(2), 2016, 442.

⁵⁰ M. Gal – O. Aviv, *The competitive effects of the GDPR*, cit., 383.

⁵¹ *Ibid.*, 384.

⁵² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828.

⁵³ A. Bradford, *The Brussels Effect*, cit.

⁵⁴ M. Gal – O. Aviv, *The competitive effects of the GDPR*, cit., 385.

The root cause of this misalignment, in the view of the authors, is that the impact assessment focused mostly on the comparison between the GDPR and the Data Protection Directive, thus failing to consider the impact of the GDPR on internal competition and international competitiveness in a digital environment “as the analysis disregards important aspects on the GDPR’s effects on the operation of data-based markets”.⁵⁵ This is why the authors call for “a more rigorous discussion of the inherent tension between data-based innovation and data protection”.⁵⁶

3.1.5. Indirect Costs in Terms of Restricting Data Collection and Sharing

As well captured in literature with regard to the lack of a proper evaluation of the competitive effects of the GDPR, an inherent criticism lies in the limited consideration of the costs arising from the new law in terms of restrictions on data collection and sharing.

This critique once again confirms that the approach of EU lawmakers was more sensitive to the fundamental rights dimension of data protection than to the internal market one. Also, it reflects the perception that the impact assessment was drafted “looking at the past rather than to the future”. In other terms, the Commission was mostly looking for justifications for the new measures the regulation aimed at introducing, predominantly on the basis of a comparison to the *status quo*; however, it seems to have failed to consider the in-depth influence of data protection law at such a crucial stage of evolution in technology.

This criticism comes without prejudice to the contribution that the GDPR makes (also) to enhancing the internal market dimension. The GDPR fostered legal certainty and reduced fragmentation also with a view to facilitating data flows across Europe and data transfers. However, the approach of the Commission at the stage of the proposal seems to have been one-sided as there is limited consideration of the constraints placed by the GDPR.

We find two types of constraints: compliance costs and indirect costs. While compliance costs have been explored above and our understanding is that the impact assessment largely underestimated their actual magnitude, especially in light of the emergence of compliance with data protection law as a reputational asset, indirect costs may come into play in the form of reduced ability of controllers to obtain data.⁵⁷ We considered higher costs for obtaining data and more difficult data synergies in section b) while delving into the competitive effects of the GDPR. We second the view of the authors who found that, overall, these costs also resulted in detrimental consequences, e.g., reduced contestability, in the relevant data

⁵⁵ *Ibid.*

⁵⁶ *Ibid.*

⁵⁷ See among others G. Aridor – Y. Che – T. Salz, *The effect of privacy regulation on the data industry*, cit.; C. Peukert – S. Bechtold – M. Batikas – T. Kretschmer, *Regulatory Spillovers and Data Governance*, cit., 747; G. Presidente – C. B. Frey, *The GDPR effect*, cit.

markets.

However, we think that the increasing cost of collecting personal data deserves autonomous consideration in the impact assessment, regardless of the possible competitive effects. From this perspective, we need to connect these costs to the benefits that the impact assessments estimated in terms of reduced legal fragmentation and more legal certainty. The impact assessment estimated the elimination of approximately € 2.2 billion in the administrative burden of legal fragmentation, as a result of increased harmonisation. In the assessment of compliance costs, it only included compliance costs, such as those costs deriving from DPOs designations and conducting data protection impact assessments, in addition to the administrative burdens determined by the introduction of a general obligation to demonstrate compliance with data protection law.⁵⁸ It made positive assumptions on the price of outputs as an additional category of costs and with respect to both the capacity to innovate and international competitiveness. No mention is made, however, of any costs directly or indirectly related to the restrictions imposed by the GDPR on the circulation of personal data for the sake of the strengthening of the fundamental rights dimension of data protection.

Various independent studies have shown that this is an important shortcoming of the impact assessment. These studies outlined that the GDPR was likely to introduce major obstacles for companies to engage in certain business practices based on the collection and further processing of personal data.⁵⁹ Once more, the fundamental rights “heart” of data protection seems to have prevailed over a deeper consideration of the market dimension. This is a particularly challenging aspect in light of the rise of a data-driven economy where access to data constitutes a key requirement for companies to better develop and deploy their business solutions. The advent of Artificial Intelligence (AI) shows how much data plays a key role in the development of AI systems. Supervisory authorities are currently discussing the extent to which the need for large datasets to be used in the training, validation and testing of AI systems can be reconciled with existing categories of data protection law. A key discussion⁶⁰ revolves around the identification of the proper legitimate basis for the processing activities in question. The AI Act, applying without prejudice to the GDPR, only partially ventured into these issues, providing limited guidance, in particular with respect to data governance and data quality requirements with respect to high-risk AI systems. In the meantime, legislative stances centred on the idea of data altruism, such as

⁵⁸ See GDPR & LED Impact Assessment, 77 and 152-153.

⁵⁹ See for example Deloitte, *Economic impact assessment of the proposed European General Data Protection Regulation*, 16 December 2013, which highlights the consequences on practices such as direct marketing and web analytics. See also Samuel G. Goldberg, Garrett A. Johnson, and Scott K. Shriver, *Regulating Privacy Online: An Economic Evaluation of the GDPR*, (2024) 16(1) American Economic Journal: Economic Policy 325. Other authors such as D. Geradin – T. Karanikioti – D. Katsifis, *GDPR Myopia*, cit., and M. Gal – O. Aviv, *The competitive effects of the GDPR*, cit., highlight the key impact of restrictions on data sharing and the resulting higher costs to obtain data.

⁶⁰ See the Italian Data Protection Authority temporary ban on ChatGPT adopted on 30 March 2023.

the Data Act and Data Governance Act, came up over the past few years. We can therefore question the adequacy of the traditional paradigms enshrined in EU data protection law, given the huge advantages that are connected with a large-scale use of personal (and non-personal data). The availability of more personal data, for example, could pave the way for better and more accurate AI solutions, the training of which could only derive benefits from broader and richer datasets.

All these challenges shed further light on how the GDPR impact assessment failed to consider the pivotal value of personal data as a driver for technology evolutions.⁶¹ Even if higher costs for obtaining data do not necessarily result in anticompetitive effects, they may have a negative impact on a variety of market players given the unprecedented developments in technology and the strong dependence on data.

3.2. DSA's *Ex Ante* Impact Assessment: Critical Gaps and Oversights

The DSA establishes a unified legal framework for digital services across the EU to address emerging challenges posed by online intermediaries and platforms, including those offering goods, services, and content, to EU consumers from non-EU locations.

The DSA applies to various actors, including online marketplaces, app stores, collaborative economy platforms, social media platforms, hosting services (e.g., cloud services), and intermediary infrastructure providers (e.g., internet access providers). It is an asymmetric regulation, as it provides for obligations that vary according to actors' role and size, *assuming* that these features are good proxies of the legal risks these actors entail and of their impact on users and market dynamics. All intermediaries must comply with general requirements that include establishing points of contact, transparency reporting, cooperation with legal orders, and clear terms and conditions. Hosting providers must implement further mechanisms for third-party reporting of suspected illegal content, covering the reporting of criminal activities and providing "notice and action" procedures with statements of action reasoning. In addition, for online platforms, the DSA mandates the establishment of an internal complaint-handling system, access to out-of-court dispute resolution, protections against misuse, transparency in advertising, and safety measures for minors. Finally, very large online platforms (VLOPs) and search engines (VLOSEs) are subject to additional stringent obligations, including risk management, crisis response mechanisms, independent audits, data sharing, and prohibitions on profile-based recommendations; this is due to their amplified role in the spread of illegal content and potential societal harm.

This way, the DSA acknowledges the complexity and varying nature of intermediary services (as well as of the respective providers), with a view

⁶¹ Some scholars also pointed out how the GDPR ultimately (and paradoxically) "slowed" innovation: see R. Janßen – R. Kesler – M.E. Kummer – J. Waldfogel, *GDPR and the Lost Generation of Innovative Apps*, NBER Working Paper Series, Working Paper 30038, May 2022.

to overcoming the uncertainties that emerged in national legal systems concerning the application of e-Commerce Directive.⁶² Also, the new regulation goes beyond the set of provisions enshrined in this Directive, which only governed intermediaries' liability for third-party illegal content. The DSA, instead, is a piece of legislation that is more consistent with the significant evolutions in the market of digital services that occurred over two decades. It takes account of the societal role of some of the intermediaries, namely the very-large online platforms, and the impact of their business, among others, on fundamental rights and democratic values. The transparency requirements provided by the DSA precisely reflect a deeper understanding of the implications of digital services for individuals and organisations, i.e., for society at large.

The fact that the EU lawmakers chose to replace a Directive with a Regulation, as in the case of the GDPR, is telling of the need to bring to an end the legal uncertainty sparked by the existence of 27 different pieces of legislation across the EU Member States. In particular, significant divergences emerged in the interpretation and enforcement of the liability exemptions by courts, leading to discrepancies among the various jurisdictions and, ultimately, to a decrease in the trust of consumers and organisations.

Therefore, the DSA is anticipated to provide enhanced protection and benefits across various sectors of society, addressing the needs of individuals, digital service providers, business users, and society as a whole. For individuals, the DSA strives to improve the safeguarding of fundamental rights, granting citizens more control over their online experiences. This includes easier mechanisms for reporting illegal content and reducing exposure to harmful material. Additionally, the DSA aims to bolster online safety for minors by prohibiting targeted advertisements directed at children, along with fostering transparency in content moderation decisions. For providers of digital services, the DSA is said to offer greater legal certainty through the establishment of a uniform set of laws across the European Union,⁶³ facilitating simpler compliance and enabling new startups and companies to scale more efficiently within Europe. Also, business users of digital services can benefit from the DSA, gaining broader access to EU-wide markets through digital platforms, alongside a level playing field to fairly compete against providers of illegal content. And, finally, at the societal level, the DSA introduces stronger democratic oversight and control over large, systemic platforms, ensuring that these entities are held accountable for their impact on public discourse and information. It also addresses systemic risks, such as manipulation and

⁶² For an overview of the uncertainties emerged over the past decades concerning the correct interpretation of Directive 2000/31/EC, see G.B. Dinwoodie, *Secondary Liability of Internet Service Providers*, Berlin, 2017; see also E. Apa – O. Pollicino, *Modelling the liability of internet service providers. Google vs. Vivi Down*, Milan, 2013.

⁶³ But the DSA is supposed to have a significant impact also beyond the European Union: see among others I. Tourkochoriti, *The Digital Services Act and the EU as the Global Regulator of the Internet*, in *Chicago Journal of International Law*, 24(1), 2023, Article 7, 129 and D.C. Nunziato, *The Digital Services Act and the Brussels Effect on Platform Content Moderation*, in *Chicago Journal of International Law*, 24(1), 2023, Article 6, 115.

disinformation, which pose significant challenges to democratic processes and social stability.⁶⁴

Consistent with the Better Regulation principles, the *ex ante* impact assessment leading up to the DSA mentioned these goals in relation to the rules that were to be adopted. Indeed, this document is clear and well-structured, effectively conveying to a broad audience the reasons behind the adoption of the DSA as well as its expected outcomes.

Namely, the impact assessment follows a logical, linear structure, beginning with an identification of three primary clusters of problems affecting digital markets. These are: (i) legal barriers that prevent smaller digital service providers from scaling up within the single market; (ii) societal and economic harms stemming from illegal online activities, inadequate protection of fundamental rights, and emerging risks; and (iii) ineffective supervision of digital services.

The impact assessment then explores the root causes underlying these issues, identifying factors such as legal fragmentation resulting from differing national approaches (depending on the existence of 27 different legal regimes), legal uncertainty driven by rapid technological evolution (a self-explanatory factor given that the E-Commerce Directive dated back to 2000 when most of the online platforms now regulated under the DSA did not even exist), and a lack of transparency and consistency in platforms' content moderation decisions, despite the role of public spaces of the largest among them. In addition, the impact assessment clarifies that inadequate supervision and coordination among regulatory authorities contributes to fuelling these ongoing issues.

Some of these aspects have become key in light of the growing societal impact of online platforms, such as is the case for content moderation. The shift from a perfect competition scenario to a *de facto* oligopoly in the relevant market, which has occurred in the past two decades, has contributed to strengthening the impact of the so-called "big tech companies" on shaping the public sphere, which resulted in calls for regulation even in the US.⁶⁵

Therefore, to address these challenges, the impact assessment remarks the need for a new regulation – the DSA – and its primary goals: ensuring the smooth functioning of the single market, particularly for cross-border digital services as per art. 114 TFEU, and setting a unified (and long-awaited) EU standard for content moderation. To achieve this, the impact assessment emphasises four specific sub-objectives: (a) establishing optimal conditions for the emergence and scaling of digital intermediaries

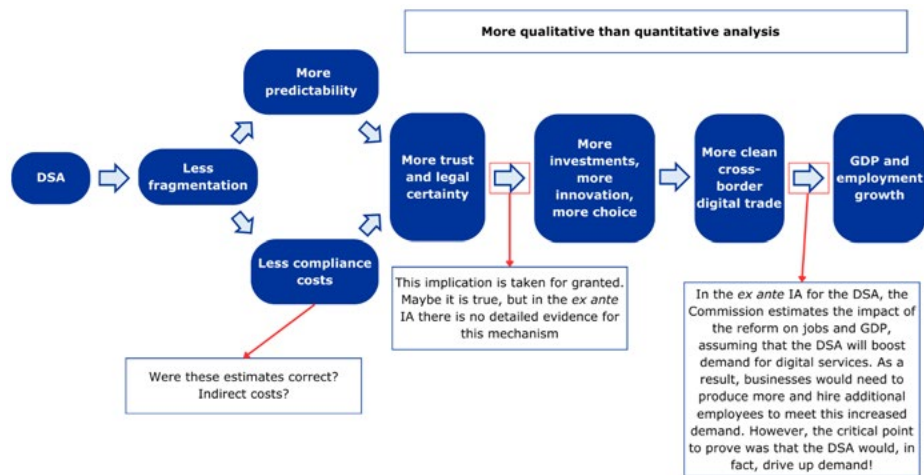
⁶⁴ For some overviews on the advantages of the DSA, see J. van Hoboken – I. Buri – J.P. Quintais – R. Fahy – N. Appelman – M. Straub (eds.), *Putting the DSA into Practice : Enforcement, Access to Justice, and Global Implications*, Berlin, 2023; M. Husovec, *Principles of the Digital Services Act*, Oxford, 2024; A. Savin, *The EU Digital Services Act: Towards a More Responsible Internet*, Copenhagen Business School Law Research Paper No. 21-04, 2021; A. Davola, *The Digital Services Act, Published: A Good Start And – Yet – Just A Start*, Kluwer Competition Law Blog, 2022; A. Turillazzi – M. Taddeo – L.- Floridi – F. Casolari, *The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications*, in *Law, Innovation and Technology*, 15(1), 2023, 83.

⁶⁵ See for example *Biden v. Knight First Amendment Institute at Columbia University*, 141 S. Ct. 1220, 1222 (2021) (Thomas, J., concurring).

within Europe; (b) empowering users and safeguarding fundamental rights; (c) ensuring a safe online environment; and (d) creating effective mechanisms for the supervision of online intermediaries. Finally, the impact assessment clarifies that, while solving the above issues, the DSA aims to uphold values that benefit not only citizens and their rights, but also economic activities conducted on and through digital platforms, ultimately supporting both consumers and businesses.

In sum, the *ex ante* impact assessment positions the DSA as a carefully designed legislative instrument to address the root causes of issues that have proven to affect the digital ecosystem. However, the impact assessment does not appear to address the expected economic impact of the DSA with the same level of detail and rigour. Namely, the impact assessment indicates that the DSA is anticipated to set off the following chain of positive outcomes.

Figure 1: The DSA's *Ex Ante* Impact Assessment



First, according to the impact assessment, the DSA is expected to reduce regulatory fragmentation, producing a double effect. On the one hand, it would lower company costs to eliminate the regulatory gaps and inconsistencies that EU firms currently face, even while they bear the expense of complying with the DSA's new rules.⁶⁶ On the other, it would increase predictability and trust through harmonised rules that promote greater legal clarity and consistency in enforcement. Reflecting on these initial “links in the chain”, one must acknowledge that the idea of harmonised rules bringing greater legal clarity—and thus more predictability—is almost self-evident.⁶⁷

However, when it comes to cost analysis, it must be acknowledged that the Commission merits credit for attempting to estimate compliance costs despite the very limited data available. Still, as always, this is a challenging task filled with assumptions. Thus, in the coming years, it will be necessary to evaluate whether these estimates prove accurate — as opposed to the GDPR, where estimates made by the EC were not accurate — and, crucially,

⁶⁶ See DSA's Impact Assessment, Table 4, 54-55 and Annex 4.

⁶⁷ See DSA's Impact Assessment, paras 177-179.

whether compliance costs will in practice be lower than those previously caused by regulatory fragmentation. The Commission assumes this will be the case—and is likely justified in doing so—but without quantifying the costs of regulatory fragmentation per company or groups of companies,⁶⁸ its observations remain more qualitative than quantitative. Amongst other findings, in its opinion, the Regulatory Scrutiny Board (RSB) found that the assessment of compliance costs outlined in the impact assessment was insufficient.⁶⁹ As a broader remark, the RSB pointed out that the evidence upon which the choice of the preferred policy option was based had to be further developed and clarified.

Second, according to the impact assessment, the DSA will increase cross-border digital trade through two complementary mechanisms: directly, because harmonised rules will make interstate commerce easier and less costly;⁷⁰ indirectly, because the induced higher levels of predictability and trust connected to the elimination of legal fragmentation will stimulate investments in EU companies,⁷¹ innovation,⁷² and thus, consumer choice. While the Commission makes considerable efforts to demonstrate the DSA's direct impact on cross-border trade using a specific empirical model,⁷³ it does not elucidate the mechanisms by which trust and certainty would lead to increased investment and, more critically, fails to clarify how and to what extent such investment would foster innovation—especially successful innovation sufficient to enhance consumer choice. Interestingly enough, the DSA seems to have a more visible impact on consumer trust, as a number of provisions provide for a significant empowerment of users vis-à-vis online intermediaries.

Both the transparency requirements and the procedural safeguards in the DSA are very promising also in terms of increased accountability;⁷⁴ however, a direct effect on increased investments and, as a result, more innovation, is not to be taken for granted, and in any case, it is

⁶⁸ Indeed, when discussing the costs of legal fragmentation, the Commission focuses primarily on the impact that legal fragmentation has on cross-border traffic rather than on the income loss that companies incur.

⁶⁹ European Commission, Regulatory Scrutiny Board opinion, *Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*, SEC(2020) 432, 6.11.2020. The main critical points raised by the RSB concerned: i) the lack of sufficient explanations concerning the coherence between the DSA and the sectoral legislation and the role of self-regulation; 2) the incomplete and underdeveloped nature of the policy options, found to lack detail and not well explained, 3) the lack of evidence leading to the choice of the preferred policy option and the insufficient assessment of compliance costs.

⁷⁰ See DSA's Impact Assessment, para 180.

⁷¹ *Ibid.*, para 182.

⁷² *Ibid.*, para. 183. To be sure, the Commission affirms that «by cutting the costs of the evolving legal fragmentation [the first option among the three under analysis will allow] services to repurpose resources in growing their business and, potentially, investing in innovative solutions». However, this effect can be attributed also to the third option that the Commission chose as the bases of the current DSA.

⁷³ See DSA's Impact Assessment, Annex 4, 56-61.

⁷⁴ See for example J.P. Quintais – N. Appelmann – R. Ó Fathaigh, *Using Terms and Conditions to apply Fundamental Rights to Content Moderation*, in *German Law Journal*, 24(5), 2023, 881.

not demonstrated in the impact assessment. In particular, from reading paragraphs 184 to 186, it appears that, by eliminating legal fragmentation, the DSA will provide businesses with greater confidence and this, in turn, will reduce the fear of inadvertently violating the law, which will encourage them to experiment more, ultimately leading not only to more services offered to both other businesses and consumers but also to an “increase in e-commerce, in particular cross-border, including positive impacts on the creative industry, manufacturing, information service and software, etc”.⁷⁵ Conceivably, these implications may indeed materialise in practice, although in the *ex ante* impact assessment, the Commission paints them with a broad brush. Yet, a truly evidence-based analysis would support such claims with relevant literature, elucidate the mechanisms producing these effects, and provide estimates of their scope. Without these elements, the assessment remains qualitative rather than quantitative.

But there is more to consider. In the impact assessment, the Commission affirms that the DSA will trigger an increase in the EU GDP.⁷⁶ To show this result, the Commission employs the input-output model to evaluate the DSA’s impact on economic growth. Input-output models offer a simplified perspective on the interconnections between various sectors of the economy. They take the form of matrices, with different industries represented in both rows and columns and allow studying what happens to the variables of the model when one of them changes. The Commission clearly outlines such transmission mechanisms in Annex 4 of the impact assessment of the DSA. It considers an increase in demand for online sales driven by government policies addressing consumer protection, explaining that this demand surge will lead e-commerce websites to procure more items from wholesalers or manufacturers. As a result, manufacturers will need to hire additional workers to boost production, as well as logistics firms to deliver items to consumers, thereby indirectly increasing overall employment. Additionally, manufacturers will require more raw materials and intermediate goods and services for the manufacturing process. As they purchase more intermediate goods and services, the producers of those inputs will respond to increased demand by hiring more workers and acquiring additional resources. Overall—the Commission concludes—the rise in e-commerce sales leads to a direct increase in total employment due to e-commerce websites hiring more personnel to manage the higher demand, along with indirect increases in employment from other producers in the value chain.⁷⁷

Thus, to frame the impact of the DSA on economic growth, the Commission replicates this reasoning, by correctly arguing that if demand for cross-border digital services rises, businesses will need to scale up production and hire more staff to meet this demand. However, in the example of e-commerce websites, the Commission assumes—without providing an explanation—that a government policy addressing consumer protection will lead to increased demand for online sales. Similarly,

⁷⁵ See DSA’s Impact Assessment, para 186.

⁷⁶ *Ibid.*, para 189.

⁷⁷ See Annex 4, 66.

regarding the DSA, the critical point that needs to be substantiated is not merely that an increase in demand for cross-border digital services triggers a rise in the supply of those services; this is a relatively straightforward implication. The EC should demonstrate that the DSA would actually drive up demand in the first place. Yet, the impact assessment fails to do this, as the Commission somehow acknowledges when it states that, “[i]n this case, the figures underlying the estimation depend on the assumption that a revised policy for illegal content online will bring more certainty and confidence to users, which in turn will translate into greater expenditure in e-commerce and increased usage of other digital services”.⁷⁸

In light of this, we suggest that to address uncertainties regarding the DSA’s potential to foster economic growth and job creation, an *ex post* impact assessment should provide empirical evidence to verify whether the DSA’s goals are being realised in practice. Specifically, such an assessment should examine whether the DSA has effectively increased demand for digital services by fostering a safer, more trustworthy digital environment, which, in turn, should attract more investment and lead to greater consumer engagement and trust. It should further investigate whether enhanced trust and safety have helped businesses to scale across the single market and if increased legal certainty has promoted innovation and broadened consumer choice.

Additionally, the *ex post* evaluation should assess whether the compliance costs associated with the DSA are manageable, ensuring that its implementation does not unduly burden digital service providers. This overview should also include the role of digital service coordinators, i.e., the bodies designated in every Member State to monitor and enforce the obligations under the DSA.

3.3. DMA’s *Ex Ante* Impact Assessment: Areas for Improvement

The DMA aims to foster fair and competitive digital markets by addressing the power of large online platforms. These companies, known as “gatekeepers”, hold considerable influence as intermediaries between businesses and consumers, controlling access to key digital services and holding entrenched market positions across several scenarios. The objective of the DMA is hence to ensure that gatekeepers operate fairly, creating an online environment where both users and smaller companies can succeed without facing unfair competitive barriers, and allowing them, where possible, to challenge gatekeepers’ market positions.

Under the DMA, gatekeepers are defined as large digital platforms providing specific “core platform services”, which include online search engines, app stores, messaging services, and social networks. To qualify as a gatekeeper, a company must meet several well-defined criteria: (i) it must have a substantial economic presence across the EU and operate in multiple member states; (ii) it must connect a large user base with a

⁷⁸ *Ibid.*

wide range of businesses, highlighting its intermediary role; and (iii) its market position must be longstanding, demonstrating that its influence has become entrenched over time.

To regulate gatekeepers' behaviour, the DMA specifies (or would like to specify) clear obligations and prohibitions, setting a framework for acceptable conduct and curbing practices that could undermine market contestability and be unfair. Among the key obligations, gatekeepers are required to: (i) allow third-party platforms to interoperate with their services in certain cases, which fosters a more interconnected digital ecosystem and enhances user choice; (ii) grant business users on their platform access to their own data, enabling better business decisions and optimised strategies based on accurate data; (iii) equip advertisers and publishers with tools and data to independently verify the performance of their advertisements, which promotes fair competition by preventing gatekeepers from manipulating ad metrics; and (iv) allow business users to promote their services and enter into contracts with customers outside the gatekeeper's platform, giving businesses greater control over their customer interactions.

The DMA also tries to outline specific prohibitions for gatekeepers. For example, they are (i) prohibited from favouring their own products and services over those of third parties in rankings or other visibility methods, levelling the playing field and allowing competitors fair access to consumers; (ii) restricted from blocking consumers from connecting with businesses outside the platform's ecosystem, thus supporting consumer choice; (iii) prevented from pre-installing or restricting the removal of software on users' devices, safeguarding user autonomy and device customisation; and (iv) barred from tracking users outside of their platform without explicit consent, which protects user privacy and curtails opaque targeted advertising practices.

Thus, through these provisions, the DMA is intended to bring substantial benefits to consumers, businesses, and the EU's digital ecosystem as a whole. According to EU institutions, business users dependent on gatekeepers will find a more equitable environment in which to operate. Previously, smaller companies faced restrictive conditions that stifled their growth potential. With the DMA, these companies could conduct business on more balanced terms, giving them a fair opportunity to compete. For innovators and technology start-ups, the DMA is said to offer relief from the barriers to entry and growth traditionally imposed by dominant platforms. Without restrictive conditions, start-ups are free to experiment, innovate, and bring new services to market without fear of being unfairly restricted. In the view of EU institutions, consumers also stand to gain significantly, enjoying a broader range of services, more options to switch providers, and fairer pricing. The DMA obligates gatekeepers to make it easier for consumers to explore alternatives, fostering competition and improving service quality across the market. Furthermore, from the perspective of the drafters of the DMA, while gatekeepers are restricted from certain monopolistic practices, they are encouraged to continue innovating—though without using unfair practices that disadvantage their business users or customers. Additionally, the DMA aimed to introduce

new levels of legal clarity for these platforms because, for the first time, gatekeepers should face clearly defined obligations they must adhere to, so that non-compliance could even result in significant penalties or even structural changes within the company, such as asset divestiture.

Structured similarly to the impact assessment for the DSA, this DMA impact assessment systematically identifies clusters of key issues, examines their underlying causes, and proposes potential solutions. This sequence not only delineates the problem areas but also reveals the values the Commission is committed to safeguarding.

The impact assessment begins by categorising issues into three main problem clusters. First, it identifies the high barriers to market entry, entrenched platform dominance, weak contestability, high digital market concentration, substantial mark-ups, and limited competition. Second, it addresses the power imbalance where platforms impose unfair conditions on business users, manifesting through anti-steering provisions, exclusive data control, restricted access and interoperability, and self-preferencing. Third, it highlights the fragmented regulatory environment, which has increased compliance costs, fostered regulatory shopping, and hindered uniform oversight.

Next, the impact assessment connects these issues to several root causes. It attributes the first cluster to market inefficiencies arising from entry barriers and cognitive biases among users. The second stems from cases where business users are economically dependent on gatekeepers, while the third is linked to legal fragmentation, as shown by the diverse national laws regulating platforms.

The assessment ultimately identifies the DMA's overarching objective: ensuring the proper functioning of the internal market by promoting effective, contestable, and fair competition in digital markets. To achieve this, it emphasises the need to address market failures, mitigate unfair conduct, and enhance both enforcement consistency and legal clarity.

This framework thus highlights two main insights. First, through the DMA, the Commission aims to protect essential legal interests: a competitive market structure, the vitality of fringe competition, business pluralism, fairness (viewed as enabling consumers and businesses alike to benefit from the platform economy), and the integrity of the single market. Second, the impact assessment presents the DMA as a targeted legislative tool, crafted to address the root causes of the identified challenges directly and systematically.

The impact assessment, however, reveals several critical issues. Some critical points already emerged in the RSB opinion, which only after an initial revision of the document became positive with reservations.⁷⁹

Firstly, it illustrates the challenges posed by regulatory fragmentation

⁷⁹ European Commission, Regulatory Scrutiny Board opinion, *Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)*, SEC(2020) 437/2, 19.1.2021. The second opinion, delivered on the revised version of the report, identified two main shortcomings, namely: 1) the absence of a justification for the selection of the core platform services to be covered by the proposal; and 2) the lack of sufficient definition of some of the measures included under the different policy options considered in the impact assessment.

and examines the use of art. 114 TFEU as the legal basis for the DMA. The cross-border nature of digital products and services, combined with independent regulatory actions by Member States, has led to regulatory inefficacy, fragmentation, and legal uncertainty. Thus, an EU-level intervention is deemed necessary, aligning with the principle of subsidiarity, to ensure harmonised regulation across the Union and to minimise associated costs.⁸⁰ Nevertheless, the assessment does not address the potential advantages and disadvantages of alternative legal bases, such as arts. 103 or 352 TFEU. Moreover, the DMA would leave existing national laws unchanged, and it would not significantly restrict Member States' ability to introduce new rules that may conflict with those established by the DMA. Additionally, the DMA lacks coordination with other EU laws applicable to gatekeepers.

Consequently, when estimating the DMA's costs, the impact assessment overlooks the implications of "regulatory layering" —that is, the accumulation of DMA rules atop other pre-existing European (e.g., the GDPR) and national regulations (e.g., rules addressing abuse of economic dependence), as well as those introduced concurrently, such as the DSA or art. 19a of the German Competition Act (GWB). The costs of regulatory layering, which encompass both compliance burdens and increased legal uncertainty, are paradoxically the same costs the DMA aims to alleviate.

Secondly, the DMA is portrayed as a solution to the enforcement shortcomings of EU competition law,⁸¹ because it clearly identifies the firms it governs without the need for case-by-case analysis and explicitly defines both unlawful practices and the specific obligations of gatekeepers. However, the emphasis on the DMA's clarity seems overestimated. The regulation consists of a complex set of rules that require interpretation, making it overly optimistic to assume that its application will not incur significant costs, including litigation. On the contrary, the DMA could introduce significant legal uncertainty, which in turn may increase compliance costs, as repeated requests for changes by regulators incur engineering costs. It could also affect how innovation is deployed by gatekeepers. This may result in certain platforms and enabling technologies reaching European business users and consumers more slowly, thereby impacting their ability to compete in global markets, and distorting competition in adjacent

⁸⁰ Paras. 100-107 of Part 1 and in Annexes 5.4 and 5.5.

⁸¹ On a theoretical level, the DMA is also presented as a solution to various shortcomings of antitrust law. It is argued that the DMA limits other forms of power, such as disposal power; redistributes resources and opportunities between gatekeepers and their competitors; and aims to reduce information asymmetries affecting businesses and end users of digital platforms. Additionally, it seeks to limit the bargaining power of gatekeepers and prohibit their one-sided practices to ensure fairness in digital markets, while also lowering barriers to entry to enhance market contestability. While this perspective is valid, it is important to note that EU competition law primarily addresses market power and does not aim to guarantee equal resources and opportunities for all market participants. EU competition law accepts initial firm endowments as given. Furthermore, antitrust rules consist of prohibitions enforced retrospectively, leaving several competitive issues unaddressed, such as consumer biases, exploitation of superior bargaining power, fairness, barriers to entry, and market contestability. Thus, the so-called "failures" of EU competition law do not arise from its inherent gaps or inconsistencies; rather, they stem from the fundamental nature of competition law itself.

markets.

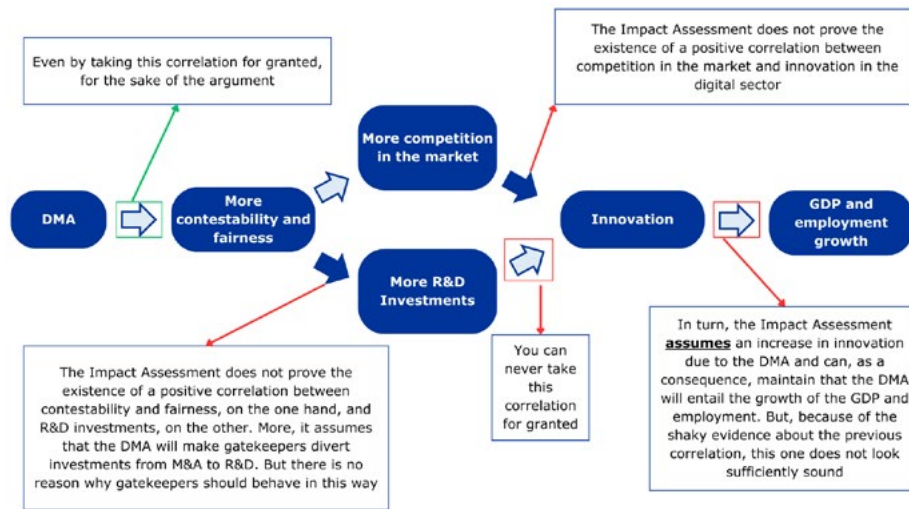
Thirdly, the impact assessment indicates that the rules established by the DMA prohibit practices previously identified as anti-competitive in both national and European antitrust cases.⁸² Yet, antitrust law is inherently fact-specific—conduct deemed harmful in one market context may not necessarily be so in another. The Commission itself recognises this complexity, noting that antitrust investigations are time-consuming because they necessitate a thorough assessment of the effects of specific conduct within its market context. As a result, the fact that a practice adopted by a company with a particular business model has been deemed anti-competitive in a specific market with certain competitive dynamics does not necessarily mean that the same practice will be anti-competitive if undertaken by a company with a different business model operating in a market with different dynamics. Consequently, two pertinent questions emerge: (a) is it appropriate to regard a prior antitrust case as compelling evidence of harm to competition? One might contend that what constitutes anti-competitive behaviour in one market (pertaining to a particular business model) may not apply in a different market (related to an alternative business model); and (b) should the Commission not have demonstrated that the practices prohibited under the DMA consistently, or at least in the majority of cases, lead to higher prices and/or diminished quality and innovation?

Fourthly, the impact assessment may not have sufficiently considered the implications of the DMA on platform integrity and security, which could incur indirect costs—either for gatekeepers, who may face the challenge of managing new integrity issues or for consumers and business users, who may be exposed to increased risks.⁸³

Finally—and perhaps most critically—the projected economic impact of the DMA appears insufficiently substantiated. Much like the impact assessment for the DSA, the DMA's assessment constructs a sequence of anticipated effects to justify how the regulation will ultimately stimulate growth in the EU economy.

⁸² Annex II.

⁸³ See ENISA 2024 Cyber Threat Landscape, 64, reading «IBM reports, throughout 2023, an average cost of 4.67M USD for a data breach with Business email compromise as the initial attack vector. Social Engineering as an initial vector is reported as having an average cost of 4.55M USD in general. Phishing in general was reported as most prevalent attack vector (16%) and the second most expensive at USD 4.76M USD» and 71, stating «[a]ccording to the Cost of a Data Breach Report 2023 the average total cost of a data breach increased to USD 4.45 million in 2023, with a total increase of 15.3% since 2020 and a continuous increase since 2017 (except for 2020)».

Figure 2: The DMA's *Ex Ante* Impact Assessment

It begins with an implicit assumption that the new rules will be effective in reducing unfair practices and increasing market contestability. Consequentially, it asserts a dual outcome: enhanced competition *in* the market (and not *for* the market) and increased R&D investment. This, in turn, is expected to spur innovation,⁸⁴ ultimately leading to growth in both employment⁸⁵ and the EU's GDP.⁸⁶

However, even assuming the DMA's effectiveness, the impact assessment falls short in demonstrating a positive correlation between increased contestability and fairness, on the one hand, and greater R&D investment on the other. Additionally, it presumes that the DMA will lead gatekeepers to shift investment from M&A activities toward R&D,⁸⁷ though no clear

⁸⁴ Without EU's intervention «[i]nnovation would remain concentrated within a small number of gatekeepers, ultimately limiting consumers' possibility to access innovation and data-friendly services provided by a larger number of platforms than gatekeepers» (para 98 of the impact assessment). Furthermore, the EC quotes several papers of distinguished scholars showing that competition (and not market concentration) spurs innovation (para 279).

⁸⁵ (1) Competition boost employment growth; (2) The IA support Study shows that the DMA's regulatory corrective measures will create thousands of additional jobs (paras 292-293).

⁸⁶ (1) «several empirical studies confirm that more competition on markets results in higher productivity in affected industries, which translates into economic growth. Other studies also confirm the positive effects of competition on the productive efficiency of companies due to (i) 'between-firms' effect, by which better companies succeed while the worst ones fail and leave the market, and (ii) a 'within-firm' effect by which companies in competitive environments are better managed» (para 275). (2) «business users argue that unfair practices would lead to up to 15% loss in their sales» (para 276). (3) In Annex 4: to «incorporate the impact of market contestability and fairer competition in GDP and employment into the [input-output] model, we needed to assume that such market dynamic would result in higher investment in R&D in the platform economy, impacting in GDP and job creation» (para. 69).

⁸⁷ The IA support study shows that «financial resources that could be invested in R&D are diverted to mergers and acquisitions, which results in higher market concentration instead of increase in the quality and quantity of products and services for consumers. The pattern of innovation dedicated to competing 'for the market' has a detrimental effect on consumer choice and surplus» (paras 282 and 322).

rationale supports this behavioural shift. Moreover, the assumption that heightened competition directly fosters greater innovation remains contested. The debate between Arrow's view, which links competition with innovation, and Schumpeter's opposing view is still active. While the Commission references the U-shaped model to suggest that a certain level of competition—not necessarily a plurality of firms—is needed to drive innovation, this model is not specific to digital markets. Similarly, the notion that increased R&D investment directly translates to heightened innovation is overly simplistic; conditions under which this link holds true should be specified to ground it in evidence. Finally, the underlying assumption that greater innovation will lead to economic growth is overextended and not fully substantiated. The impact assessment relies on an input-output matrix to argue that an innovation boost, catalysed by the DMA, will drive GDP and employment growth. Yet this matrix merely illustrates that GDP and employment might rise when specific positive changes are made to any influencing variable; it does not establish causation.⁸⁸

Overall, in light of what has been said so far and the possible future improvements mentioned, the *ex post* evaluation should aim to clarify several uncertainties surrounding the justification for how the DMA could drive economic growth and job creation. Specifically, it should provide supporting evidence regarding whether the DMA effectively makes markets more contestable and fair, increases competition in digital markets, enhances innovation, boosts overall R&D investments, and contributes to GDP and employment growth. Additionally, the assessment should demonstrate that, following the DMA's prohibition of certain practices, markets that no longer engage in those practices experience lower prices and greater innovation. Finally, it should illustrate that, as a result of the DMA, instances of multiple proceedings and decisions have been reduced.

3.4. Summarising Key Findings from our Analysis

The Commission's *ex ante* impact assessments are thoughtfully crafted, effectively outlining how the adopted rules aim to address specific factors identified as root causes of well-defined problems. The principles behind these rules—whether safeguarding fundamental rights or promoting fairness in business relationships—are conveyed with clarity, making them not only legitimate but also widely reasonable and acceptable.

However, these assessments are less compelling when it comes to detailing the economic impact of the new rules. In particular, they fall short in precision and depth in the following areas:

- Direct compliance costs, with significant underestimations of both their magnitude and sources.
- Potential indirect costs, such as missed business opportunities and effects on competitive dynamics.

⁸⁸ D. Teece – H. Kahwaty, *Is the Proposed Digital Markets Act the Cure for Europe's Platform Ills? Evidence from the European Commission's Impact Assessment*, BRG Institute, 2021.

- Assumptions about positive outcomes, like the assertion that “greater trust leads to increased demand”, which are presented as self-evident truths.
- Claims regarding broader economic benefits, including projected boosts to GDP and employment attributed to the laws.

In other words, when drafting its impact assessments, the Commission is convincing in outlining the values it seeks to uphold and the legal interests it aims to protect through proposed laws. Consider, for example, the focus on the protection of fundamental rights in the GDPR and the DSA, the attention paid to fairness, contestability, and business pluralism in the DMA, and the always-present goal of market integration.

However, the Commission demonstrates less precision when detailing the economic impact of these new rules. While it occasionally provides empirical evidence and references economic models, this approach is neither systematic nor consistently thorough. In particular, there are not only inconsistencies in the cost estimates associated with these new rules, but some of the cause-and-effect mechanisms or strong correlations that these rules are meant to trigger or refer to appear to be taken for granted. As a result, there is a clear opportunity for improvement. *Ex post* evaluations could serve as a valuable tool for filling these gaps, providing the public with the necessary evidence to evaluate the true economic effects of the laws.

4. Ex-post evaluations

4.1. Methodologies for Evaluations

Next to robust *ex ante* impact assessments, *ex post* evaluations are just as – or even more – important, as they study the real impacts of EU legislation. This is why each EU law generally foresees an evaluation, to be done by the European Commission, three or four years after its entry into force and periodically afterwards.⁸⁹ Sometimes, the legislator instructs the Commission to evaluate specific issues, often because these issues were contentious during the legislative negotiation. This is the case, for instance, for the imposition of interoperability obligations amongst social networks as provided by the DMA.

Evaluations are particularly important for the new EU digital acquis because, on the one hand, the legislations are new and therefore some unintended effects may not have been anticipated in the impact assessment, and on the other hand, digital industries are dynamic, innovative, and complex (and not yet fully understood). Indeed, as noted by the Council of the OECD in its Recommendation on agile regulatory governance:⁹⁰

«In light of the regulatory challenges raised by innovation, undertaking a shift in regulatory policy processes will be essential,

⁸⁹ Art. 97, GDPR; art. 91, DSA; art. 53, DMA.

⁹⁰ OECD, *Recommendation of the Council for Agile Regulatory Governance to Harness Innovation*, OECD/LEGAL/0464, 9.

whereby the traditional “regulate and forget” mindset must give way to “adapt-and-learn” approaches. The capability to detect and understand innovations and their potential impact on existing regulations, or, more important, the public values that are at stake, is key. Addressing any “pacing problem” requires, in particular, shortening timeframes throughout the policymaking process and using regulatory management tools in a more dynamic, adaptive and iterative manner. In this new paradigm, stakeholder engagement, regulatory impact assessment (RIA), and *ex post* evaluation should not be seen as a series of discrete requirements to be conducted successively, but rather as mutually complementary tools embedded in the policy cycle to inform the appropriate adaptation of regulatory (or alternative) approaches».⁹¹

4.1.1. Dimensions to Evaluate

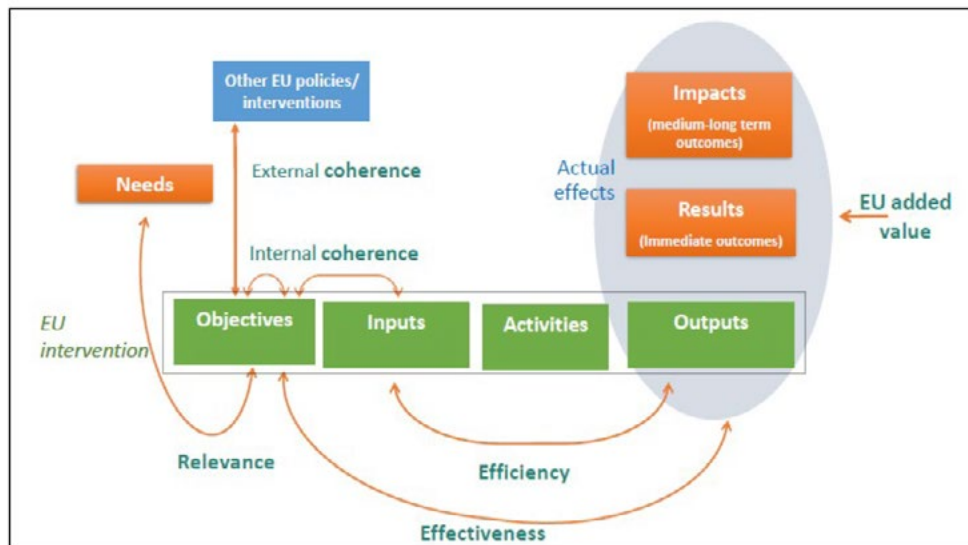
According to the European Commission Better Regulation Guidelines,⁹² an *ex post* evaluation should be an evidence-based assessment along five dimensions, determining the extent to which the EU law:

1. is *effective* in fulfilling expectations and meeting its objectives (which implies that the objectives of the law are clearly identified), this includes an analysis of the unexpected and unintended effects;
2. is *efficient* in terms of cost-effectiveness and proportionality of actual costs (including administrative and adjustment costs) to benefits, this includes an analysis of possibilities of simplification and reduction of inefficiencies;
3. is *relevant* to current and emerging needs;
4. is *coherent* internally (i.e., within the same legal instrument) as well as externally with other EU interventions and international agreements; this includes the identification of tensions and synergies among regulatory instruments;
5. and has *EU added value*, i.e., produces results beyond what would have been achieved by Member States acting alone.

The Better Regulation Guidelines clarify that the evaluation goes beyond an assessment of *what* happened; it also considers *why* it happened (the role of the EU intervention) and, if possible, *how much* has changed.

⁹¹ This is referred as back-to-back evaluation and impact assessment as Tool 50 of the Commission Better Regulation Toolbox.

⁹² Better Regulation Guidelines SWD(2021) 305, 23 and Tool 47 of the 2023 Better Regulation Toolbox.

Figure 3: Simplified view of the evaluation⁹³

When several laws are evaluated together, the evaluation could be done through a more comprehensive fitness check to determine the coherence of the various laws and seek to quantify any synergies (e.g., improved performance, simplification, lower costs, reduced burdens) or inefficiencies (e.g., excessive burdens, overlaps, gaps, inconsistencies, implementation problems, and/or obsolete measures) over time. This would help identify the cumulative impact of the interventions, in terms of costs and benefits. More specifically for the tech sector, which is key for European competitiveness, the Draghi Report underlines the importance of applying three principles:

- First, the principle of *simplification* in order to strike the right balance between the principle of precaution and the principle of innovation;
- Second, the principle of *proportionality* in order not to over-regulate the SMEs and small mid-caps;⁹⁴
- Third, the principle of *consistency in the enforcement* across the single market in order to facilitate cross-border operations and the scale-up of tech firms.⁹⁵

Given the importance of those three principles, they should be evaluated carefully for the DMA. In particular, the Draghi Report recommends a revamped competitiveness test, merging the existing competitiveness test and SME test⁹⁶ to measure the cumulative impact on SMEs of EU regulation with a clear and strong methodology, including both compliance costs and administrative burden. As seen above, this recommendation has now been integrated in the mission letter of Executive Vice-President Virkkunen.

⁹³ 2023 Better Regulation Toolbox, 405.

⁹⁴ The principle of proportionality is a constitutional principle in EU law: art.5(4) TEU.

⁹⁵ Draghi Report, cit., Part B, 322-326.

⁹⁶ Those two (currently separated) tests are explained in Tools 21 and 23 of the Commission Better Regulation Toolbox.

4.1.2. Features of a Good Evaluation

The Commission Better Regulation Guidelines note that the evaluation should be independent and objective, i.e., based on all relevant information, conducted without influence or pressure by third parties and report transparently on the positive and negative elements of the analysis.⁹⁷

Moreover, the Better Regulation Guidelines also note that the evaluation should be based on the best available evidence drawn from a diverse and appropriate range of methods and sources (triangulation).⁹⁸ This implies an identification of indicators and data in order to conduct a robust evaluation along the five dimensions and then the collection of the data as soon as the new law enters into force.⁹⁹

To improve the quality of evidence and deal with all the data effectively, the OECD recommends capitalising on technological solutions.¹⁰⁰ Indeed, Big Data and AI technologies provide substantial opportunities to improve the evaluation of EU laws. As shown with the use of SupTech by financial supervisors,¹⁰¹ they can be helpful for (i) data collection and significantly improve reporting, virtual assistance, and data management as well as (ii) for data analytics and enhance market surveillance, misconduct analysis, and prudential supervision.¹⁰² More ambitiously, SupTech could also be used for market evolution simulation with agent-based computational modelling.¹⁰³

For innovative sectors like tech, the OECD also recommends developing adaptive, iterative, and flexible regulatory assessment cycles. Indeed, the evaluation process should evolve over time as more information on the impact of a law becomes available and as the evaluator improves indicators, data, and processes. Also, evaluation should lead to adaptation, corrections, and improvements of the law.

⁹⁷ Better Regulation Guidelines SWD(2021) 305, 26.

⁹⁸ *Ibid.*

⁹⁹ As noted in Tool 46 on designing evaluation of the Commission Better Regulation Toolbox, the JRC or external sources may be useful to identify and collect the relevant indicators.

¹⁰⁰ OECD Recommendation on Agile Regulatory Governance, 6.

¹⁰¹ For an overview of the suptech used by financial supervisors, see the [database of the Cambridge SupTech Law at the Cambridge Judge Business School](https://ccaf.io/suptechlab), in ccaf.io/suptechlab, as well as the [Bank of International Settlement \(BIS\) Innovation Hub](https://bis.org), in bis.org. Next to regulators, the antitrust authorities are also exploring the use of big data and AI to improve their operations: T. Schrepel – T. Groza, *The Adoption of Computational Antitrust by Agencies: 2021 Report*, in *Stanford Computational Antitrust*, 2022, 78 and the [Computational Antitrust project](https://lam.stanford.edu) in lam.stanford.edu.

¹⁰² S. di Castri – S. Hohl – A. Kulenkampff – J. Prenio *The suptech generations*, Financial Stability Institute Insights, 2019, 19.

¹⁰³ As suggested by W.B. Arthur, *Foundations of Complexity Economics*, in *Nature Review: Physics*, 3, 3021, 136.

4.2. Specific Digital Laws

Of the three laws analysed in this report, only the GDPR has been evaluated by the European Commission, both in 2020 and then in 2024. The DMA will be evaluated for the first time in May 2026 and the DSA in February 2027 (with some specific issues having to be evaluated beforehand).

4.2.1. GDPR

The 2020 evaluation of the GDPR by the Commission¹⁰⁴ is fairly positive, noting that: (1) citizens are more empowered and aware of their rights, (2) businesses - including SMEs - have one set of rules to comply with, and (3) the risk-based and technology-neutral approach does not impede innovation. In terms of improvement, the evaluation notes that it is necessary to support a harmonised and consistent implementation and enforcement of the GDPR across the EU, which led to the Commission proposing a new Regulation to ensure stronger enforcement of the GDPR in cross-border cases.¹⁰⁵

The 2024 evaluation¹⁰⁶ notes that the GDPR has empowered people by allowing them to have control over their data. It has also helped create a level playing field for businesses and has become a cornerstone of the EU digital acquis. However, there is a need for (1) proactive support for stakeholders by data protection authorities in their compliance efforts, especially SMEs; (2) a consistent interpretation and application of the GDPR across the EU, as well as a robust enforcement of the GDPR with the rapid adoption of the Commission's proposal on procedural rules to deliver quick remedies and legal certainty in cross-border cases; (3) effective cooperation between regulators at both national and EU level to guarantee the consistent and coherent application of the growing body of EU digital rules; and (4) further advancing the Commission's international strategy on data protection.

However, those two Commission reports were more qualitative assessments of the beginning of GDPR implementation instead of fully-fledged and rigorous evaluations following the Better Regulation Guidelines. In particular, the reports do not really address the issues of effectiveness and efficiency, nor do they mention the study of the GDPR on innovation, in particular from tech the perspective of start-ups. This is problematic given the increasing academic empirical literature showing the possible effects of the GDPR for SMEs, in particular where Member States add national rules to the EU rules, ("gold-plating") as recalled in the Draghi Report.¹⁰⁷

¹⁰⁴ *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation*, COM(2020) 264 and SWD(2020) 115.

¹⁰⁵ *Commission Proposal of 4 July 2023 for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation 2016/679*, COM(2023) 348.

¹⁰⁶ *Second Report on the application of the General Data Protection Regulation*, COM(2024) 357.

¹⁰⁷ Draghi Report, cit., Part B, 319.

The Commission reports study the (lack) of consistency in enforcement and the effects on tech scale-ups and tries to propose remedies more in that regard.

4.2.2. DSA and DMA

Given that the DSA and the DMA have just been enforced, they have not yet been evaluated. However, the process for a robust and independent evaluation should already be prepared now.

Regarding *robustness*, it is key that the relevant indicators are specified to assess the effectiveness and efficiency of these two important EU laws which, in turn, require determining their objectives with precision.

Once those indicators have been specified, a strategy for data identification and collection should be designed. The data could be sourced from (i) the regulated platforms,¹⁰⁸ in particular through their new transparency obligations (such as the compliance reports under the DMA or the systemic risk assessment reports under the DSA), (ii) their business or end-users, (iii) the EU bodies and regulatory networks (such as the Joint Research Centre of the European Commission which monitors the effect of the digital transition,¹⁰⁹ or the EU regulatory networks in charge of specific policies like ENISA for network security, ECN for competition policy, the CPC Network for consumer protection, or BEREC for electronic communications services), (iv) academic or civil society research which ideally should be mapped out by the Commission as part of the evaluation process or (v) if necessary additional surveys. As recommended by the OECD, the collected data should also be processed and analysed with AI tools when relevant.

Regarding *independence*, the Commission is in charge of the evaluation (as is the case for other EU laws). There is however a risk of conflict of interest as the Commission is also the enforcer of the DMA (totally) and the DSA (partially). To be sure, the Commission often procures the preparatory work for an evaluation from external consultants, yet these consultants are not necessarily independent when considering they regularly have to bid for new contracts with the Commission. The draft evaluation report of a Commission service is also reviewed by the Regulatory Scrutiny Board, who does an independent quality control, yet this Board is also part of the Commission and not immune for internal influence.

Therefore, it would be preferable that the DMA and the DSA are evaluated by a body which is fully independent from the Commission. One possibility would be the European Court of Auditors which sometimes carries out performance audits for specific EU policies besides its main role of auditing EU finances.¹¹⁰ Given that one of the strategic areas of

¹⁰⁸ Respecting the principle of proportionality as well as the rules on intellectual property, trade secrets and confidentiality.

¹⁰⁹ *Digital transformation, cybersecurity - Digital transformation: technologies, cybersecurity and socio-economic impact*, in joint-research-centre.ec.europa.eu.

¹¹⁰ European Court of Auditors Methodological Guide 2023, 18-24. For instance, the Court recently adopted an interesting (and critical) [report on the EU Artificial intelligence](#)

focus of the Court is EU economic competitiveness,¹¹¹ of which the tech sector is a key component, it would make sense that it contributes to the evaluation of the DMA and the DSA. For this, the Court should develop and rely on specific expertise in the tech sector and adopt a pragmatic – and not formalistic tick-the-box – approach to the evaluation.

Another possibility, which can be complementary, would be the appointment on a merit basis of a panel of high-level independent experts by the European Parliament and the Council. One interesting previous example is the inter-disciplinary team of top-level academics which wrote in 2019 the Report on Competition policy for the digital era.¹¹²

To increase the independence, the draft evaluation report of the Commission should also subject to a meaningful public consultation.

5. Policy Recommendations

5.1. General Recommendations

We should recognise the opportunities of the *ex ante* and *ex post* assessments in improving policy making by being more evidence-based and having a better understanding of the relationships between rules, firms and users conduct, and users benefits. However, we should also recognise their threats when assessments are retro-engineered to achieve pre-determined policy options, or when quantification of policy options are not possible or even misleading. Also, these assessments should remain proportionate and not inappropriately delay the policymaking process, nor should they become a substitute for political decisions within the democratic decision-making process.¹¹³ Below, we make policy recommendations on substance and process to maximise those opportunities while minimising the threats.

5.1.1. Recommendations on Substance

1. Identification of Causality Links and Policy Trade-Offs

The main added value of the *ex ante* and *ex post* assessments is to identify the causality links between (1) the rules and the incentives they created, (2) the conduct of the firms, their competitors, their consumers, or citizens, and (3) the users benefits.

Thus, those main causal relationships should be clearly identified in the *ex ante* impact assessment and justified by relying on the best, most suitable evidence and models available in the academic literature. This involves clearly outlining the “transmission mechanisms” through which rules are expected to produce a chain of effects, each dependent upon the other. The Commission should avoid assuming certain links and should explicitly

ambition, in *eca.europa.eu*, 2024.

¹¹¹ The 2021-25 strategy of the European Court of Auditors, in *eca.europa.eu*.

¹¹² *Shaping competition policy in the era of digitisation*, in *competition-policy.ec.europa.eu*.

¹¹³ Interinstitutional Agreement of 13 April 2016 on Better Law Making, point 12.

clarify when these links represent cause-and-effect relationships and when they merely indicate correlations.

The validity of the causal relationships established in the impact assessment between the rules, the conduct of firms, and resulting consumers benefits should be revisited in the *ex post* evaluation, when the effects of the laws are evident in real market data and the rules should be corrected if needed. Another important added value of the assessments is to identify trade-offs associated with the various policy options which may differ, i.e.: (i) *economic* between regulation, competition, and innovation; (ii) *non-purely economic* between different fundamental rights (iii) *institutional* between EU and national level of intervention; or (iv) regarding *regulatory design* between symmetric or asymmetric rules, or between horizontal or vertical rules. The different effects of those trade-offs may also unfold in a different time frame. For example, positive short-term price effects may have longer term costs in terms of innovation, or more complex consumer choice may have more long-term benefits in terms of innovation.

In particular, security risks should be thoroughly considered in the process of assessing policy trade-offs, in line with the European Commission's objective to achieve "security-by-design" policymaking.¹¹⁴ In this vein, the Niinistö report on EU preparedness and readiness called on the EU to develop a mandatory "security and preparedness check" for future impacts assessments, in the context of the Better Regulation toolbox.¹¹⁵

The Commission should undertake a holistic cost-benefit analysis that weighs regulatory objectives against the potential long-term impact on digital ecosystem dynamics, taking into account differing timelines for costs and for benefits, as costs are often frontloaded, while benefits usually take time to be realised. This assessment should take into account the cumulative effect of multiple regulatory burdens on gatekeepers, with particular attention to the risk of stifling the very mechanisms that make digital ecosystems successful in the first place.

The *ex ante* impact assessments should clearly identify in a qualitative manner the main types of trade-offs and, when feasible, have a quantitative assessment of those trade-offs. Subsequently, the identification and the quantification of those trade-offs should be revisited in the *ex post* evaluations with real market data.

2. Identification of Indicators and Data

Once the main causal relationships and policy trade-offs have been identified, the next step consists of identifying and collecting the necessary indicators and data to measure those relationships and trade-offs. These measurements should be done using the best available data, especially sourced from independent and high-quality academic studies, or should be complemented by additional research done for the Commission. A lot of the necessary data is likely to be compiled by firms, so the EU legislators should ensure that rules include reporting obligations to enable a proper *ex post* evaluation.

¹¹⁴ As set out in the European Commission's 2024-2029 Political guidelines (15)

¹¹⁵ S. Niinistö, *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*, in *commission.europa.eu*, 2024, 55.

Often a precise quantification will be impossible, especially for the impact assessments which are forward-looking. In this case, precise numbers should be avoided as they could be severely misleading, and orders of magnitude should be preferred.

3. Dynamic Regulatory Assessments

As recommended by the OECD, the traditional “regulate-and-forget” mindset must give way to a dynamic “adapt-and-learn” approach. *Ex ante* impact assessment and *ex post* evaluation should not be seen as a series of discrete requirements to be conducted successively, but rather as mutually complementary tools embedded in the policy cycle to inform the appropriate adaptation of regulatory (or alternative) approaches. Therefore, *ex post* evaluations should test the assumptions on which the impact assessments were based, and if some assumptions turn out to be incorrect, the laws need to be adapted. Moreover, each new evaluation should be built on the previous evaluations, taking into account newly available market data, and correcting mistakes from past evaluations. Finally, each evaluation should lead to concrete recommendations for lawmakers to follow up upon.

4. Attention to Regulatory Consistency

While in the early days the EU digital acquis consisted of light touch regulations that introduced relatively minimal rules to allow the internal market to function, they have over time grown more dense and complex, and they focus not only on establishing the internal market, but also on enhancing fundamental rights, safety, consumer protection, competition, resilience, or environmental sustainability. With the increasing complexity and technicity of the regulatory framework, we see a growing risk in overlapping - or even conflicting - regulations, accompanied by an increasingly complex compliance and enforcement framework. Therefore, we think it is key that in future impact assessments and evaluations pay more attention to the interplay between new laws with existing – or parallelly proposed – laws.¹¹⁶ Potentially, a codification exercise could positively contribute to this goal.

5.1.2. Recommendations on Process

5. Robust and Independent Assessment Process within the European Commission

The process of *ex ante* and *ex post* assessment within the European Commission should guarantee robustness and independence. To do that, we recommend that the draft impact assessment and evaluation report should be subject to a public consultation before their analysis by the Regulatory Scrutiny Board. This will allow all interested stakeholders, which have access to better information and data than the Commission, to give their views on the identified causal relationships and policy trade-offs, as well as on the use of indicators and data; the interested stakeholders may also propose alternative indicators and data.

¹¹⁶ As mentioned in the mission letter of EVP Virkunnen.

Taking into account the outcome of the public consultation, the Commission services should revise their draft impact assessment or evaluation report and explain in a separate document how the outcome of the consultation has been taken into account. For the draft impact assessment, the Commission may also run a sensitivity analysis on the causality assumptions with the information gathered, to demonstrate outcomes and if some assumptions differ from the “base case” as small variations in assumptions may lead to significant changes of policy impacts. With all this information, the Regulatory Scrutiny Board could improve its quality control of the causality and trade-offs identified, and the use of indicators and data in the impact assessment and evaluation. In case of a negative opinion by the Regulatory Scrutiny Board, the Commission services should in principle adapt not only the assessment but also the legislative proposal. The opinion of the Regulatory Scrutiny Board as well as the changes made to the impact assessment and the legislative proposal should then be made public after the adoption by the College of Commissioners.

Specifically, for the *ex post* evaluations, the content and process of the evaluations should be carefully prepared as soon as a new law is in force. In particular, the indicators that will be evaluated and the data that will be collected should be determined early on and big data and AI technologies may contribute to the collection and analysis of the data. Also, an independent evaluation should be designed, taking into account the risk of conflict of interest where the Commission is at the same time enforcing and evaluating a law.

6. Stricter adherence to impact assessments throughout the entire law-making process: a “life cycle” approach to Better Regulation

In order for *ex ante* impact assessments to provide real added value in the preparation of new legislation, it is essential to develop mechanisms to ensure that they are seriously taken into account during all stages of the legislative process, given the possible discrepancies between the assessment made by the Commission in the impact assessment at the time of a proposal’s publication and the final text of a legislative act.¹¹⁷ At the same time, a more evidence-based impact assessment can result in more robust proposals that can more easily overcome political bargaining and fulfil their initial “commitment”.

This would imply, as already foreseen by the Interinstitutional Agreement of 2016 on Better Law-making,¹¹⁸ that the impact of any substantial amendment to the Commission proposal introduced by the European Parliament or the Council should be assessed by the institution tabling it, possibly with the support of the Commission. In turn, this would require a strengthening of the role of the policy assessment services within the Parliament (Directorate for Impact Assessment and Foresight within

¹¹⁷ See also Draghi Report, cit., Part B, 324.

¹¹⁸ Interinstitutional Agreement of 13 April 2016 on Better Law Making, points 15-17. The mission letter of Dombrovskis states that he should «lead the negotiations on a renewed inter institutional agreement on simplification and better law making. This should ensure that each institution assesses the impact and cost of its proposals and amendments in the same way with a simple and clear methodology».

the EPRS) and the Council. This may also require the introduction of a mechanism allowing the Commission and the EU legislator to request an assessment of any new scope or obligations and pause negotiation until the assessment is available.¹¹⁹

5.2. Recommendations for Specific EU Digital Laws

5.2.1. GDPR

1. Conduct a Comprehensive Assessment of Compliance Costs

It is key that the EU institutions understand the pivotal value that compliance with data protection law has gained for organisations based in the EU and outside the EU. While transitioning from the Data Protection Directive to the GDPR could make it difficult to assess the practical impact of the changes in legislation, it is recommended that future developments and amendments in the GDPR strictly adhere to the status quo in terms of evaluation of the actual impact of obligations and requirements.

2. Conduct a Deeper Review of the Overall Effects of the GDPR

In a data-driven society where “data is the new oil”, a holistic understanding of the multi-faceted implications of the governance and regulation of personal (and non-personal) information is required. The GDPR impact assessment seems to have underestimated the peculiar structure and features of data markets, thus failing to take into account possible unintended consequences, causing an impact from the perspective of competition law. The adoption of the GDPR was followed by a series of legislative actions (such as the Digital Markets Act, the Data Act, the Data Governance Act) directly or indirectly concerning data markets and data sharing practices. It is recommended that future developments in the evaluation of the provisions and mechanisms behind the GDPR take full account of this broader context to more carefully calibrate the relevant impacts.

3. Evaluate the Impact of the Restrictions on Data Sharing in a Data-Driven Economy

The provisions empowering individuals in their capacity as data subjects have a key role in increasing consumers’ trust in the digital economy. However, data play a pivotal role in a data-driven economy where technological advancements such as Artificial Intelligence technologies progressively rely more on the ability to collect and share data. It is therefore recommended that the value of data to society as a whole is fully taken into account in future assessments, in the search of a fair and reasonable balance between privacy protection and the promotion of innovation.

¹¹⁹ Similar to the existing possibility to request an opinion from the legal services.

5.2.2. DSA

4. Conduct a Comprehensive Assessment of Compliance Costs

The European Commission should carry out an evidence-based evaluation to determine whether compliance costs linked to the DSA are indeed lower compared to those resulting from past regulatory fragmentation. The assessment should focus on quantifying compliance costs, particularly for SMEs, to ensure that obligations are proportionate and manageable. Empirical data and relevant studies should be leveraged to substantiate claims and elucidate the mechanisms driving cost reductions.

5. Evaluate Economic Growth and Demand-Enhancing Mechanisms

To address uncertainties regarding the DSA's potential impact on economic growth and employment, the *ex post* impact assessment must verify if the DSA has effectively increased demand for digital services by creating a safer and more trustworthy online environment. The evaluation should assess whether these changes have led to increased consumer engagement, investment, business scaling within the EU single market, and greater market opportunities for companies.

5.2.3. DMA

6. Address the Costs of Regulatory Layering

The *ex post* impact assessment of the DMA should thoroughly evaluate the cumulative impact of regulatory layering, which results from the interaction between the DMA and other European and national laws. This assessment should specifically address the compliance burdens and legal uncertainties created by the overlap between the DMA and other complementary laws, such as the GDPR, DSA, and national laws like the German Competition Act. A clearer understanding of these costs will help identify whether the DMA has successfully alleviated regulatory fragmentation or inadvertently added complexity to the regulatory landscape.

7. Evaluate the Real-World Clarity and Application of the DMA

The *ex post* assessment should critically examine the practical application of the DMA, considering its complexity and the need for interpretation. It should investigate whether the Regulation's clarity has been overstated in the *ex ante* analysis, particularly with regard to the costs incurred by businesses and legal entities in understanding and applying its rules. The assessment should also evaluate the extent to which the DMA has led to litigation or compliance challenges, and whether the expected simplification of the regulatory environment has materialised in practice.

8. Provide Empirical Evidence on the Consistency of Anti-Competitive Practices

The *ex post* evaluation should assess whether the practices prohibited under the DMA are indeed consistently anti-competitive across a broad range of markets and business models. This analysis should go beyond relying on prior antitrust cases and demonstrate with empirical evidence that the behaviours addressed by the DMA universally lead to higher prices, reduced quality, or less innovation. By evaluating the consistency and scope

of anti-competitive effects in various market contexts, the assessment can determine whether the DMA's prohibitions are appropriately targeted or overreaching.

9. Strengthen the Evidence Base for Projected Economic Impact

The *ex post* impact assessment of the DMA should rigorously evaluate the actual economic outcomes resulting from the Regulation, with a particular focus on substantiating the causal links between increased market contestability, enhanced competition, and growth in R&D investment. The assessment should provide empirical evidence to support or challenge the assumptions made in the *ex ante* analysis, especially regarding the relationship between competition and innovation in digital markets. It should also assess whether the DMA has effectively shifted investment towards R&D and away from mergers and acquisitions, as anticipated. Furthermore, the Commission should clarify the conditions under which increased R&D leads to meaningful innovation and economic growth, ensuring that these claims are grounded in market-specific evidence rather than generalised theoretical models. Finally, the *ex post* evaluation should reconsider the underlying assumption that innovation will inevitably lead to GDP and employment growth, providing a more nuanced analysis of how these factors interact in practice within the digital economy.

Abstract

This paper critically addresses the application of the Better Regulation principles within the European Union's evolving legislative framework for the digital economy and evaluates the effectiveness of this framework in addressing the economic and societal impacts of the digital transformation. Focusing on three major pieces of the EU digital rulebook, i.e. the General Data Protection Regulation (GDPR), the Digital Services Act (DSA) and the Digital Markets Act (DMA), the paper provides recommendations to improve the *ex ante* and *ex post* regulatory assessments in order to ameliorate the digital rulebook and ensure that the EU can regain its competitiveness and promote responsible innovation, while protecting EU values and fundamental rights.

Keywords

Better Regulation principles – EU Digital law – European digital competitiveness – Brussels effect – digital economy