SVENSKT NÄRINGSLIV
SWEDISH ENTERPRISE

New regulations in Europe's digital economy

DESIGN, STRUCTURE, TRADE, AND ECONOMIC EFFECTS

JUNE 2023

Authors: Matthias Bauer, Fredrik Erixon, Oscar Guinea, Philipp Lamprecht, Vanika Sharma, Renata Zilli

Contents

Foreword 2

Executive summary 3

1. Introduction 5

2. The Digital Markets Act 8
- 2.1 What is the Digital Markets Act? 8
- 2.2 Legal basis, subsidiarity, and proportionality 10
- 2.3 How does it work? 11
- 2.4 The potential impact of the regulation 12

3. The Digital Services Act 15
- 3.1 What is the Digital Services Act? 15
- 3.2 Legal basis, subsidiarity, and proportionality 16
- 3.3 How does it work? 17
- 3.4 The potential impact of the regulation 19

4. The Artificial Intelligence Act 22
- 4.1 What is the Artificial Intelligence Act? 22
- 4.2 Legal basis, subsidiarity, and proportionality 23
- 4.3 How does it work? 24
- 4.4 The potential impact of the regulation 26

5. The Data Act 30
- 5.1 What is the Data Act? 30
- 5.2 Legal basis, subsidiarity, and proportionality 31
- 5.3 How does it work? 32
- 5.4 The potential impact of the regulation 33

6. Analysis of the impact on markets and trade policy 37
- 6.1 Market and trade analysis 37
- 6.2 Trade policy analysis 44
- 6.3 Risk of retaliation 53

7. Conclusion 57

Foreword

Time to map and analyse the impact of the EU's digital regulations

In recent years, the European Union has become increasingly active in regulating data and the digital economy. Since 2014, the European Commission has taken several steps to establish a digital single market through a large number of new acts, including those considered by this report:

- the Digital Markets Act, which aims to establish fair and contestable markets for innovation, growth, and competitiveness in the digital sector.
- the Digital Services Act, which is designed is to create a safer digital space where the rights of all users of digital services are protected.
- the Data Act, which regulates access to data in B2B, B2C, and B2G (business-to-government) relationships and while switching between cloud providers.
- the AI Act, which enacts stringent regulations of (high-risk) AI systems and prohibition of certain practices.

Businesses are concerned by the many new digital regulations and are calling for action to boost competitiveness and create regulatory breathing space. By any measure, the EU is introducing a very significant wave of new regulation. It is clear that these new digital acts – individually and as a whole – will have a substantial impact on most economic actors that work with data and compete in the digital economy, which effectively includes virtually all business of all sizes today. In addition, the impact of digital regulations on trade and trade policy are routinely neglected in the proposals and the Impact Assessments.

The Confederation of Swedish Enterprise has commissioned the European Centre for International Political Economy (ECIPE) to map and further analyse the four acts. This is done in two deliverables. This first deliverable will focus on the design, structure, trade policy effects and economic effects while the second deliverable will map the quantitative impact on trade flows.

The observations and recommendations of this study are intended to help policy-makers and other relevant stakeholders to shape the digital future of Europe. When doing so, Europe's competitiveness should be a top priority. New initiatives must include further engagement with industry to better identify, understand and address future initiatives and their potential impacts.

Stockholm, June 2023

Karin Johansson
Vice President Confederation of Swedish Enterprise

Executive summary

In recent years, the European Union has become very active in regulating data and the digital economy. To address specific concerns and generally to develop technological and digital autonomy in Europe, the European Commission has launched scores of new regulations that individually and collectively will have a strong impact on Europe's digital economy. This report aims to shed light on four new digital regulations – the Digital Markets Act, the Digital Services Act, the Artificial Intelligence Act, and, finally, the Data Act. The report analyses the purpose, structure, and design of the regulations, and reviews the quality of the regulatory process – especially the extent to which the Impact Assessments provided adequate contextual and economic analysis. Additionally, the report seeks to map potential frictions between the digital regulations and EU commitments in international trade agreements – issues that were largely absent in the Impact Assessments of the four regulations.

The report does not give an outright judgment of the four regulations but there are some general conclusions that can be drawn.

- All four regulations are complex. The objectives are often not clearly defined, and concepts used in the regulations – for example how they define "data", "data holder", and "artificial intelligence" – are ambiguous and prompt more questions than they give answer. The regulation assumes that later regulatory processes (for instance, through the work of standardisation bodies) will help to define and make regulations more operable. While standards are incredibly important and helpful, there is much that standards cannot achieve and that must be clearly defined or decided by legislators. Overall, the EU should make greater efforts to provide less complex regulations and be clearer in how its objectives are reflected in the regulatory provisions.
- The Impact Assessments of all four regulations are inadequate. While it is difficult to provide context and deep economic analysis of complex regulations – and of complex economic phenomena – it is obvious that the assessments have neglected important areas of the regulations. The economic analyses in the Impact Assessments, or accompanying reports, are incomplete. They exaggerate benefits and come to conclusions, for instance on GDP effects, that are very unlikely. Moreover, the assessments routinely find administrative and implementation costs to be remarkably low. There is a wealth of economic analyses of previous regulations that could help provide more realistic economic estimations of the effects. The conclusion we draw is that, because of inadequate analyses, legislators are flying in the dark about the reasonable economic effects of regulations.

- Better economic analysis and higher standards in the Impact Assessments are important for two other reasons. First, legislation often changes between the tabled proposal and the final version of a new regulation, and the EU could benefit substantially by having more opportunities for evaluation – in addition to presenting more solid analysis at the time when a proposal is made. Second, the four regulations will all have a substantial impact on the same services, data, companies, investments and trade flows. Several regulations overlap and their combinatory effects are likely to be considerable – which motivates not just analysis of one single proposal but of several proposals.
- Trade and trade policy are routinely neglected in the proposals and the Impact Assessments. Given that digital services are of strong importance for the European economy, and that the EU is competitive and runs a significant trade surplus in these services, such neglect goes against Europe's economic interest. Notably, the debate surrounding the four regulations often starts from the presumption that Europe should be defensive because it lacks international competitiveness. A more careful approach would accommodate the fact that new regulations can impact Europe's international competitiveness and reduce its trade surplus.
- Some of the new digital regulations are clearly discriminatory as they exclude some providers of digital services – as, for instance, in the Digital Markets Act and the Data Act. Even if it is not de jure discrimination, it is obvious that there are considerable frictions between effective discrimination and EU obligations in the World Trade Organisation (WTO). While the relevant WTO agreement allows for departures from rules and obligations, these departures are conditional and the rules to obtain approval to discriminate will be awkward for the EU, if another country decides to press it on WTO compliance. A better impact assessment could have helped to alleviate some of these frictions and made the proposals compliant with the EU's international obligations.
- Many of the new regulations have consequences for the protection of trade secrets and other intellectual property rights. This can be a minefield. The structure of protection of assets and investments in the intangible economy is different from the tangible economy. Companies mix various forms of protection, including contracts, in order to have a model that gives sufficient motivations to make investment in data and digital services, and sharing them with others. Some of the new regulations, especially the Data Act, can upend this system of protection and erode trade secrets. It is highly advisable that the legislator develop a much deeper understanding of the consequences of such initiatives before they are made.
- The effects of the four digital regulations are geographically concentrated. It is predominantly services and service suppliers from the US that will be affected. This clearly raises the risk of retaliation – in the same way as the US moved for retaliation against EU countries introducing new digital services taxes. If the effect is diffused on many countries, there is less likelihood of retaliation. If the effects are concentrated, the risks of retaliation increase substantially.

1. Introduction

In recent years, the European Union has introduced many new policies with the effect of regulating data, its use, and the broader digital economy. Following the General Data Protection Regulation (GDPR), which took effect in 2018, new EU regulations have come thick and fast. Moreover, new regulations have often been different than traditional regulations in the past, which typically focused on regulating products and their potential risks for consumers and the environment. Now they are more prescriptive and cover wider structures of supply and production, and they aim at outcomes that go beyond the usual scope of regulation. While the stated motivations for the regulation may have varied, observers have noted a new EU ambition to emerge as a global superpower in digital regulation. It is also clear that these regulations are part of a general ambition to lead the EU towards technological and digital sovereignty.

New regulations on digital markets and digital services were initialled in the autumn of 2022 – the so-called Digital Markets Act and the Digital Services Act. Some other proposals for new regulations have been processed in the past year, and they include the Artificial Intelligence Act and the Data Act. These two regulations are expected to be adopted in 2023, perhaps already in the first half of the year. A new Cybersecurity Act has been in force since 2019 but there are now proposed additions to this with the EU Cybersecurity Certification Scheme for Cloud Services and the EU Cyber Resilience Act. A new version of the Network and Information Security Directive is also making its way through the EU decision making process.

By any standards, this is a very significant wave of new regulation, and it is reasonable to expect the new policies to have a significant impact on most economic operators who work with data and compete in Europe's digital economy. It is less clear, however, that there is a good understanding of how these regulations are intended to work in practice – or what their impact will be on companies and various aspects of their value chain (let alone the wider economy) over time. It appears that many companies struggle to grasp how specific regulations will force change in their operations. Moreover, as many regulations overlap with each other and address the same companies, assets, and behaviour, there is even greater uncertainty about their combined effect. Therefore, it is safe to say that there is considerable demand for understanding the design and operation of these regulations, and how they will impact the EU economy and Europe's relations with other parts of the world.

While some of these new regulations and proposals build on existing regulations, others are novel and chart a new course for Europe's digital economy. Even if there is a global trend of regulations of data and the digital economy, many new regulations operate in territories where there are few precedents that can help to shed light on the operation and effects of them. Furthermore, it is notable that the impact assessments

that have accompanied many of these new regulations in the EU have been thin on economic analysis. As has been noted by the EU's Regulatory Scrutiny Board in several instances, the design of the new regulations is sometimes difficult to comprehend, and it is often unclear how the regulations will impact on their stated objectives.

This is unfortunate. All new regulations face similar challenges. For a regulation to be successful, it should be based on clear objectives and go through rigorous scrutiny in impact assessments that help to make the regulation clear, understandable, and effective. This is critical for achieving good outcomes and avoid unintended consequences: distinct and clearly communicated regulations are easier to work with for those who are affected by them. However, some regulations face more challenges than others, and this is especially the case for many of the new regulations that go to the heart of innovation and target complex technology, like Artificial Intelligence (AI). Regulators are then confronted with matters that are difficult to place in a conventional model of regulation. Moreover, the effect of a regulation can be extraordinarily powerful because it works with frontier technological development and market change. The risk is that a poorly designed regulation will have an outsized negative impact on the economy.

Therefore, international organisations frequently push governments to improve the quality of regulation.[1] In the past, unclear objectives and inadequate frameworks for implementation have often caused unnecessary economic, social, and environmental harm. Therefore, guidelines and principles from organisations like the OECD, the World Bank and the WTO aim to make regulations "fit for purpose". For instance, the OECD says that "clear objectives and frameworks for implementation" are critical for the efficiency of a regulation. Moreover, it also suggests "drafting and adopting regulation through evidence-based decision-making" and the use of external "mechanisms and institutions to actively provide oversight of regulatory policy procedures and goals".[2]

In this study, we review four new digital regulations – and we are doing so with the assistance of established principles for good regulation. The four regulations are the Digital Markets Act, the Digital Services Act, the Artificial Intelligence Act, and the Data Act. The purpose of these analyses is to obtain a better understanding of how these regulations will work in practice and how they will impact the economy, especially trade. The intention of the analysis is not to pass a general verdict whether the regulations are motivated or not – let alone whether they should be adopted or rejected. While this study is primarily based on qualitative analysis, a quantitative analysis of these regulations will be provided in a forthcoming study.

It is important to better understand the effects of new digital regulations on Europe's trade. Europe is a relatively open economy with significant trade and investment relations in the global digital economy. Many European exports are powered by data-based services and Europe generally has comparative advantages in the digital

[1] The following section draws on OECD (2020) "Cracking the code: Rulemaking for humans and machines", OECD Working Papers on Public Governance, No. 42. OECD (2020) Regulatory Impact Assessment. OECD. World Economic Forum (2020). Agile regulation for the fourth industrial revolution: A toolkit for regulators. WEF.

[2] OECD (2012) Recommendation of the Council on Regulatory Policy and Governance. OECD (2012) Regulatory reform and innovation.

economy. Furthermore, Europe is increasingly dependent on accessing technologies and digital services that were not invented in the region, and the competitiveness of economies, firms and individuals rely on their ability to work with the best available digital technologies and services. The digital economy is a highly globalised economy with substantial volumes of trade and investment. Cross-border data flows are crucial for the performance of many services, and at the heart of the competitive performance of firms are human capital flows. European firms are increasingly organising their digital operations in global teams, and with significant shortages in advanced labour the trend towards management, staff and operational globalisation has accelerated. In other words, it is of vital importance for Europe's economic growth that new digital regulations build on knowledge about how they will impact on Europe's dense cross-border linkages.

Unfortunately, trade and cross-border consequences have not featured in impacts assessments and other economic analysis that have accompanied these regulations. This is surprising, to say the least, considering the extent of Europe's relations with the outside world. But such analysis is crucially important because many new digital regulations have provisions that clearly have consequences for how European firms and users link up with their foreign partners, suppliers and customers. Thus, an enlightened discussion about these regulations requires a better understanding of how international economic relations are likely to be affected.

Furthermore, if there are strong impacts on partner economies, they may decide to take retaliatory action against the EU, and it is important to better understand whether and how such actions could be designed. The political economy of the cross-border effects seems obvious. Many of these regulations will disproportionally affect companies and sales in one country – the US. On the export side, however, Europe's digital economy is more diversified, and retaliatory actions would not be as concentrated as the cross-border impacts on third countries.

More specifically, this study analyses:

1. The objectives and the design of the regulations.
2. The practicalities of the regulations: how will they work?
3. The quality of the regulatory process.
4. The impact of the regulations on the EU's international trade (which flows could be impacted).
5. The compatibility of the regulation with rules in international organisations and in international agreements signed by the EU.
6. The retaliatory risk of the regulations.

The study is structured as follows. The next four chapters (Chapters 2–5) will include an analysis of each of the four regulations. In this analysis, we will review the objective and the intended operation of the regulations and consider whether the impact assessments included relevant economic aspects of these regulations. In other words, this analysis will include points 1–3 in the above list. Chapter six will consider different international aspects of these regulations (points 4–6 in the list), especially the specific consequences for trade policy. The last chapter concludes the paper with some summary observations and recommendations for the future regulatory process.

2. The Digital Markets Act

2.1 What is the Digital Markets Act?

The Digital Markets Act (DMA) is a new regulation, adopted in the autumn of 2022, that aims at regulating the behaviour of large platforms – so-called "gatekeepers", most likely companies such as Amazon, Apple, and Google. The act builds on the economics of competition policy and decades-long expert and academic discussions on "ex ante" and "ex post" competition policy – and the efficiency of traditional competition approaches in fast-moving sectors that is heavily influenced by the logic of two-sided network markets. However, it is equally clear that the motivation for the DMA draws on political considerations outside the scope of competition policy and a general desire to make major platforms conform to EU ambitions for them and the markets where they operate. Therefore, it is a stretch of imagination to say that the DMA is anchored in the objectives, concepts, and instruments of traditional ex-post competition policy. A more accurate description is that the DMA is a firm-specific regulation with ambitions to re-shape sectoral market regulations.

The DMA aims at promoting competition, contestability, and fairness, and the regulation occasionally makes references to objectives such as consumer protection and innovation. Its underlying assumption is that gatekeepers have entrenched and durable market positions which give them substantial market power and an opportunity to act in ways that reduce competition and fairness. It builds on the proposition that market developments in some digital services in the past decade have given too much market power to large platforms, and that competition policy is inadequate to address uses and abuses of that market power.

A large platform, for instance, can deny access to other providers of digital services or set the terms for access in such a way that is unfair to a third-party provider. As a result, competition will be reduced as platform users will be denied the chance to choose between many good competing alternatives. Since consumers can be locked into platforms, or face high switching costs between platforms, the Commission argues that there should be new rules of behaviour for platforms that conform to the interest of the consumer. Without such rules, consumer choice and innovation will be severely handicapped.

A novel aspect of the DMA is that the regulation is firm specific. While the regulation aims at re-shaping markets to provide for better competition, contestability, fairness, consumer protection and innovation, it does not provide horizontal rules that are

applicable to the market and to all operators in a specific market. The rules in the DMA are only applicable to those firms who will be covered by the DMA – the so called "gatekeepers".

Gatekeepers, or their designation in the DMA, are defined on the basis of certain criteria. First, gatekeepers are defined by their "core platform service", and the DMA covers most services that are associated with the large platforms: online intermediation services, online search engines; online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating systems, cloud computing services, advertising services, web browsers, and virtual assistants.

Second, for a core platform service to be covered by the regulation, a company will be designated as gatekeeper if its size and operation exceed certain thresholds. These threshold criteria are: 1) its annual turnover in the EU is more than €7.5 billion or its market valuation is greater than €75 billion; 2) it has more than 45 million active monthly end users or 10,000 active yearly business users in the EU; and 3) has exceeded the second criteria in the past three financial years. The third criterion is the threshold test for having an entrenched and durable market position.

There are two sets of rules in the DMA: obligations and prohibitions that are either prescriptive or proscriptive, or "dos" and "don'ts". The list of dos is long and includes mandatory rules for interoperability and allowing users, for example, to uninstall pre-installed services. Many of these prescriptive rules are modelled on cases that involve smart phones and various digital services – provided by the smart phone producer and third parties – that are connected to the device, apps, store, and contract functions. For instance, user-generated data from the device platform should be accessible for a third party provided with users on the platform, and they should be able to contract and use payment facilities that are outside of the device platform and unconnected to any specific platform rules.

The don'ts, or the prohibitions, include rules that affect more types of platform services, and consequently has bigger reach and effect on platforms, users, and markets. Article 5 of the DMA starts with four very specific prohibitions on the use of certain data. First, the gatekeeper is banned from processing data, for the purpose of online advertising services, from personal end users who use a third-party service on the platform. Second, a gatekeeper is banned from combining personal data from the core platform service with personal data from any other core platform service or from any other service provided by the gatekeeper. Third, a gatekeeper is banned from cross-using personal data from the core platform service in other services provided separately by the gatekeeper. Fourth, the gatekeeper is banned from signing in end-users to other services of the gatekeeper in order to combine personal data.

Even if the designation of the gatekeepers has not been done yet, many observers have pointed to a number of platforms that are highly likely to receive such designation. On that basis, it is also possible to observe that many platforms services that are currently operated by platforms will be affected by the DMA. These effects are likely to lead to significant amendments in the operation of services and what platforms can offer to their consumers. The DMA may also lead to some specific services being terminated.

There are other prohibitions in the DMA as well. For instance, there is a ban on self-preferencing, and restrictions set by the gatekeeper to prevent a user to link up with businesses outside the platform. There is also a penalty for non-compliance. If a gatekeeper is found to err with the DMA and its provisions, the Commission can impose fines of up to 10 % of the company's total worldwide annual turnover. If the violation of rules continues or is repeated, the penalty can go up to 20 % of total worldwide annual turnover plus periodic penalty payments of up to 5 % of the company's total worldwide daily turnover. In the event of systemic violation, structural remedies can be applied.

2.2 Legal basis, subsidiarity, and proportionality

The legal basis for the Digital Markets Act is Article 114 of the TFEU. While this legal basis will probably suffice – it is a "catch-all" article that empowers legislation with the intention of preventing regulatory fragmentation in the internal market – there are concepts and future practices that may sit awkwardly with the legal basis. The Commission is the sole enforcer of the DMA, but national Member States still have the power to take their own competition-enforcement measures vis-à-vis platforms that will be designated as gatekeepers. Germany, for instance, has recently updated its competition policy rules and, in a way, already have a version of a Digital Markets Act on its books. The DMA does not invalidate ex post competition policy, but the distinction between ex ante and ex post decisions is sometimes ambiguous. There is a clear risk that the same gatekeeper, core platform service and commercial practice will be subject to several and partly conflicting decisions by various authorities in Europe. Since the DMA does not prejudice competition policy and actually hands power to member state authorities, it is not clear how different actions vis-à-vis the same actor and behaviour will be addressed – if they will be addressed at all. A legal basis that is intended to reduce single market fragmentation will be difficult to square with an application of the DMA and competition policy that foments fragmentation.

Furthermore, decisions under the DMA can have an impact on other rules in the EU, for instance on privacy obligations on platforms and the protection of their intellectual property rights. It has been observed throughout the process of designing the DMA that some of the proscriptive rules in the regulation will have consequences for such rights and obligations, and that there will have to be a judgment made at some point about what rights and obligations take precedence.

Proportionality is also likely to be challenged. Building on the previous point, since the DMA does not include the right to "efficiency defence"[3] or other "objective justification" of the actions by platforms in all aspects, there could be enforcement decisions that are disproportional because they put in jeopardy other fundamental aspects and rights. In other words, there can be significant harm as a result of an

[3] In EU competition law, a company can claim that a certain practice which is allegedly a violation of core competition rules can be motivated because the efficiency gains clearly outweigh the costs. It is by no means a carte blanche for abusive market behaviour but an institution that prompts deeper economic analysis in the application of rules against abuse.

enforcement decision – for instance, an erosion of platform system integrity and cyber-security – and given the open-ended nature of the obligations and prohibitions in the DMA, such the risks of such outcomes should not be dismissed. Equally important, decisions based on market investigations that do not take into account relevant market and economic aspects of a platform could lead to substantial over-enforcement. For instance, many of the Article 5 rules have little meaning for some platforms and their users. Provisions that are designed to regulate one company, say Apple, can have little meaning for another platform, say Microsoft. Yet Microsoft has to abide by typical "Apple rules" even if "Apple behaviour" by Microsoft has no relation at all to abuses of market power.

2.3 How does it work?

The first part in the application of the DMA is the designation of the gatekeepers (described above in Section 2.1). The DMA is a regulation that only applies to a selected group of platforms and their core platform services, and it follows that the key step in the implementation of the regulation is to make this selection. By September 6, 2023, the gatekeepers will have been designated. The gatekeepers then have six months to come into compliance with the DMA. By March 6, 2024, the full force of the DMA will apply to the gatekeepers.

While the notification and decision process seem straightforward, it includes many complex issues pertaining to both the definition of a core platform service (and what a platform should notify) and the manpower capacity of the Commission to deal with complex issues in a limited period of time. There is also the prospect that a designated gatekeeper will seek to overrule the designation decision. It can be argued that it should be pretty obvious which companies that will be covered by the DMA, but it is a far less obvious matter to define what exactly constitute the core platform service and what core platform service that a gatekeeper is identified with. In fact, it is highly likely that such considerations will be so complex that, in some cases, it will be a matter for courts to make decisions.

New uncertainty emerges after a gatekeeper has been designated and the DMA provisions apply. Presumably, designated gatekeepers will use the period up to March, 2024, to work out how different provisions in Articles 5–7 will apply to their structures of business. And it is the role of the designated gatekeepers to assess the compliance. However, there will be many cases where it is difficult to exactly define what a provision entails for a certain business practice. The legislators have also stated in the DMA that some provisions (in Articles 6–7) are subject to specification, which likely means that the Commission will decide additional and detailed provisions that apply for a specific company once a gatekeeper has filed its notification or made a reasoned argument why some specific conditions must apply. The DMA also opens for the Commission to decide on changes to the provisions through delegated acts. This gives substantial discretion to the executive to tailor the rules to make them expedient to the executive and its intentions.

The Commission can also start market investigations for the purpose of designating a gatekeeper and defining the core platform service. This instrument, market investigations, will also be used for the purpose of assessing systematic non-compliance and reviewing new services and practices that will emerge. While market investigations, and other enforcement measures in the DMA, draws on competition policy, there are significant differences. The most important one is that an investigation by the Commission does not need to provide the material evidence or follow the established standard of reasoning in competition policy, supporting its decisions. The designation criteria and the provisions can apply in a direct manner, and the Commission will not need to provide supporting analysis evidencing that there is a problem resulting from the gatekeeper behaviour.

There is a final aspect to uncertainty in the application of the DMA, and it relates to the point above about risks of fragmentation in the internal market. The DMA does not supplant competition policy and national competition authorities thus have the right to take actions that go beyond the DMA. Furthermore, the DMA now also provides for the private enforcement of the DMA. In other words, a complainant can go to a national court to seek remedial action from a gatekeeper that is allegedly in violation with a DMA provision. It is likely that courts will differ in their interpretation of the DMA and what it means in complex situations. Therefore, there is likely to be fragmentation in the internal market.

2.4 The potential impact of the regulation

The impact of the DMA is likely to be substantial. The implementation and compliance costs alone are likely to exceed what the Commission has suggested by some margin. One analysis points to compliance and operational costs for US firms only in the range of $20–50 billion.[4] European business users and consumers will also be affected, leading to significant losses (€43 billion). These figures may be too high or too low, but it is remarkable that there have been so few efforts to estimate the economic effects.

While it is difficult to estimate the effects quantitatively, it is notable that the Impact Assessments that accompanied the DMA proposal were thin on economic analysis. While the Commission drew on analytical reports that it had commissioned and on outside academic studies that rightly underlined the economic risks of market concentration and platform market power, few of those were specific to what was proposed in the DMA and covered the effects they will have on users and markets. Most of the referenced studies in the Impact Assessment are rather generic and concerns issues at a conceptual rather than applied level. Notably, none of the studies that the Impact Assessment relied on concerned post-implementation evaluations of other digital

[4] These costs are both for the DMA and the DSA. Kati Sumionen (2022) Implications of the European Union's Digital Regulations on US and EU Economic and Strategic Interests. CSIS.

regulations that has been introduced in the past years in the EU. Nor did they evaluate the effects of "ex post" competition-policy decisions in the EU. After all, many of the gatekeepers have already been subject to competition enforcement and the effects of those decisions should reasonably have an influence on the design of the DMA.

The problem with providing a solid understanding of expected economic effects goes beyond concerns about irregular choices of analyses to stand on and goes to the heart the market that the EU is attempting to re-shape with the DMA. It is well established in academic and applied research that competition and market contestability – two objectives of the DMA – promote good economic outcomes. It is equally well established that two-sided markets and markets with strong network properties can lead to higher market concentration – to dominant roles for a few firms. Hence, the EU stands on solid conceptual grounds when it suggests that the DMA has economic motivations.

However, there are equally solid conceptual arguments that cast doubt on the case that the DMA is a boon to the European economy – or that DMA market interventions will foster more competition and better economic outcomes. Chief among these conceptual qualifications is the concept of networks. While the network effect of large platforms can give strong market power to a platform, it is also the case that the network effect emerges because it is beneficial to the user. In many cases, users are voluntary moving their services to one platform to save time and costs, and to benefit from the complementary effects. For instance, the platform services offered by Apple may make the Apple "ecology" difficult to contest, but for the consumer there is also a rational case for docking more online services with that ecology. Therefore, a user of a platform "ecology" derives substantial benefits from the combination of a core platform service with lots of other different services that combines data and functions of the core platform service with non-core services. Similarly, online advertisement is much better for the user if the advertiser or the provider of the online advertisement service can rely on combined and networked data. The important economic question, therefore, is how to balance negative economic network effects with positive economic network effects. This question remains unanswered. Ex-post competition policy and the type of competition economics it relies on has a method for adjudicating when market power becomes strong enough to motivate market interventions. However, the DMA will not rely on these methods.

Similarly, it is fundamentally unclear in the Impact Assessments what the substitution effects will be, and how interventions will shape dynamic aspects of competition. It seems clear that the effect of the DMA is that platforms gradually will have to reduce the usefulness of their platforms and service network. It may even be the case that some platforms will have to terminate some current services that is offered to its users. After all, the core economic essence of the DMA is that gatekeepers will be prohibited from service offerings they otherwise could provide to their customers. If that happens, and it remains unclear if it will, the question that follows is whether these aborted services will be offered by other providers and in a way that is equal to the current alternatives?

The presumption in the DMA is that such substitution will emerge naturally and that European users will not be restricted to access useful online services or that they will be saddled with poor functionality that depress the demand for an online service. However, this is questionable. Some services connected to the core platform service are of value simply because it is connected to the core platform service, and that the provider of the core platform service can offer complementary services that are useful. It may still be the case that it is economically motivated to use the DMA to prevent a platform from certain types of market offerings and competition, but it is equally important that the DMA is not used in a way that prevents European users from accessing good services that cannot be substituted in a good way. Reasonably, the Impact Assessments should have covered such aspects because they are important to Europe's digital market.

The result is that no one has a reasonably detailed estimate of how the DMA will impact on markets and users. It can turn out to be a net positive, but it can also result in net-negative economic effects for consumers in Europe.

3. The Digital Services Act

3.1 What is the Digital Services Act?

The Regulation on a Single Market for Digital Services, also known as the Digital Service Act (DSA),[5] was approved by the European Parliament and the Council on October 19, 2022. It will be directly applicable from 1 January 2024, fifteen months from its adoption, even if the implementation process has already started. The stated aim of the regulation is to ensure the proper functioning of the single market and cross-border digital services, but the scope of the regulation clearly extends beyond this specific objective. The DSA will regulate the obligations of digital platforms like Amazon and Facebook that offer services as intermediaries in connecting consumers with goods, services, and overall digital content. For instance, some of the more featured parts of the DSA concerns social media content.

The structure of the DSA is easier to comprehend than other digital regulations because it builds on the e-Commerce Directive from 2000, which has been the main policy for regulating intermediary liability in the EU. Notionally, the DSA adapts the liability regime to the modern age of digital communication – after two decades of a rapidly growing sector of platforms and platform services. However, motivation for the DSA was also based on the growing size and market power of platforms and suppliers of digital services. They will now be under stronger rules of behaviour – including rules on illegal content, access to platforms, and traceability of platform transactions. Additionally, the DSA is billed to improve online rules on freedom of speech and the general safety of any online presence.

There has obviously been an expansion in regulatory ambitions from the e-Commerce Directive to the DSA. Some of these expansions follow various conduct rules that have been agreed by the European Commission and digital platforms over the years – for instance rules on notice and takedown for illegal content – and the more economically significant aspects of the DSA are an expanded set of commercial rules on digital services.

According to the European Commission, digital services are defined as "services normally provided against remuneration, at a distance, by electronic means and at the individual request of a recipient of services"[6]. Examples of these are apps, online

[5] European Commission, 2022, Regulation 2002/2065 on a Single Market for Digital Services.

[6] European Commission, 2020, Impact Assessment for the Digital Services Act.

shops, e-games, online versions of traditional media, IoT interfaces, and payment services. The DSA specifically regulates the obligations of intermediary services, such as cloud infrastructure services, content distribution networks, app stores and social networks which represent the backbone of Internet commerce. They will face stronger responsibility to ensure that content featured on their platforms is legal and that there are established systems to control the legality and safety of content.

An expanded set of aims for the DSA, following the Commission's own presentation, therefore are:[7]

- Good conditions for innovative cross-border digital services.
- Maintaining a safe online environment with responsible and accountable behaviour from digital services.
- Empower users and protect fundamental rights and freedom of expression.
- Establish supervision of online intermediaries and cooperation between authorities.

3.2 Legal basis, subsidiarity, and proportionality

There is a clear legal basis for the DSA within EU legislation. Articles 53 and 62 of the TFEU are used as the legal bases in the domain of information services (freedom of establishment and freedom to provide services). Only the adoption of directives is permitted by these articles. The adoption of measures deemed necessary to bring the legal provisions closer together is based on Article 114. The legal basis is solid.

Likewise, the DSA builds on precedence: the e-Commerce Directive has a legal foundation for the freedom of establishment and freedom to provide digital services in the single market. Internet services are inherently cross-border services, and the DSA attempts to overcome regulatory fragmentation within the single market. Because of this, argued the Commission, the scope of the DSA and its objectives cannot be sufficiently achieved by Member States alone. Diverging legal regimes to online platforms and intermediaries would translate into legal uncertainty and unequal protection of citizens.

The principles of subsidiarity and proportionality will govern the exercise of the EU in the DSA. Therefore, this regulation should only harmonize certain minimum conditions. Depending on the legal system of each Member State and the issue at stake, Member State authorities will order providers to act against specific illegal content.

[7] Ibid.

3.3 How does it work?

In accordance with the objectives, the DSA seeks to reform aspects of the previous E-commerce Directive by providing new information and transparency requirements on online platforms, especially very large online platforms (VLOPs), hosting services, and its intermediaries. The DSA will be directly applicable across the EU. With the exception of micro and small digital companies, all online platforms are required to publish data on the number of active monthly users by February 2023.

The DSA includes obligations for the platforms and operators that are covered in the act. It is less clear, however, how compliance with these obligations will be organised and administered. Member States will assign competent authorities and designate one authority to be the Digital Service Coordinator, with responsibility for all matters related to the application and enforcement of the DSA. This process is now under way. However, given the space for the national design and enforcement of laws and regulations related to the DSA – and that Member States have different cultures of and preferences for the regulation of intermediaries (including the use and size of penalties and other sanctions) – it is likely that countries will differ significantly in the application of the DSA and what administrative demands that are put on the covered operators. There is a substantial difference in modus operandi already between competent authorities in, for instance, Germany and Ireland on matters covered in the DSA.

Separating large platforms

The DSA creates different obligations and due diligence for online platforms based on their size. Online platforms and search engines with a number of average monthly recipients equal to or more than 45 million would be designated as VLOPs. A key part of the DSA implementation is therefore to designate the VLOPs, which was done in April 2023.

In addition to administrative requirements, VLOPs will come under new obligations, such as disclosing their algorithms to rank content and monitoring systemic risks. Likewise, the legislation includes elements of a new crisis response mechanism in cases of serious threat for public health and security, which are also only actionable for VLOPs.

The Commission will be the sole authority to oversee large online platforms, while the competence for smaller ones would fall under the designated authority of Member States.

It is clear that the Commission's intention to make a distinction between these types of platforms is to create asymmetric obligations on the basis of the role of services in intermediating content, and on their outreach to European citizens.

Table 3.1: Required due diligence in the DSA for different entities.

Required Due Diligence	VLOPs	Online Platforms	Hosting Services	All intermediaries
Points of Contact	✓	✓	✓	✓
Legal representatives	✓	✓	✓	✓
Terms and conditions	✓	✓	✓	✓
Reporting obligations	✓	✓	✓	✓
Statement of reasons	✓	✓	✓	X
Complaint handling	✓	✓	X	X
Trusted flaggers	✓	✓	X	X
Abusive behavior	✓	✓	X	X
KYBC*	✓	✓	X	X
Advertising transparency	✓	✓	X	X
Risk Assessment and mitigation	✓	X	X	X
Independent audits	✓	X	X	X
Recommender systems	✓	X	X	X
Enhanced advertising transparency	✓	X	X	X
Crisis protocols	✓	X	X	X
Data access and scrutiny	✓	X	X	X
Compliance officer	✓	X	X	X

Source: EU Commission (2021).
*KYBC stands for know-your-business-customer.

New rights and safeguards for users

The DSA introduces new "know-your-customer"-type of rules. Platforms that allow users to contract on their platforms need to verify the legality of the parties and the goods that are involved in the transaction. Hence, it will be mandatory for platforms to have in place procedures for removing illegal goods. Furthermore, there are also traceability requirements for both sellers and buyers on a platform.

Likewise, the Digital Services Act provides new safeguards for users, such as the possibility to challenge a platform's content moderation decisions when their content has been removed or restricted, the right to seek out-of-court settlements, to complain to their national authority in their own language, and to seek compensation for breaches of the rules. And in the case of minors, the DSA requires additional obligations to ensure a high level of privacy, safety, and security in the services of any online platform operating in the EU.

Moderation of illegal content

Perhaps the major novelty of the DSA is the different measures that it introduces to counteract illegal content. Users will be empowered to report illegal content, including illegal products, in an easy, user-friendly, and effective way. VLOPs will need to take mitigating measures to protect their users from illegal content, goods and services. And when enabled by national laws, Member State authorities will be able to order any platform operating in the EU, irrespective of their geographic establishment, to remove or disable access to illegal content.

This means that, under specific circumstances, the DSA can prompt platforms to act as quasi law enforcement agency and conduct independent audits, making a judgment of criminal and civil offenses by their own account, and report them if they believe there are valid suspicions of offence. In a similar fashion, VLOPs will come under new obligations to monitor "systemic risks". Systemic risk is not a defined legal concept, and it remains to be seen what it entails for enforcement.

3.4 The potential impact of the regulation

The DSA will have an impact on the operation of platforms and markets for digital services. Unfortunately, the Impact Assessment of the DSA never made an effort to map such effects and estimate their size. It is clear that the introduction of this new regulation will have a cost impact on the covered operators, who – at the very least – will have to pay for the supervisory costs. The internal compliance costs are also likely to be substantial for platforms like Facebook and YouTube.[8]

Just as with other regulations, it is highly likely that the implementation of the DSA will result in different downstream costs for businesses – platform providers as well as platform business users. Because companies vary in size and capacity, the costs are likely to vary between companies. It is not clear, however, that the economic impact on companies will be a direct reflection of their size. Obviously, VLOPs will face bigger cost burdens than smaller platforms, but smaller platforms that are growing rapidly may be confronted with a bigger impact on their business. Furthermore, on the user side, KYBC regulations are probably going to disproportionally affect micro and small businesses with little online sales. The KYBC costs for the platforms may make such business users unprofitable.

The DSA regulation could also have broader consequences for firms and resource allocation in the EU economy. And these impacts go beyond direct compliance and administrative costs. However, the Commission's Impact Assessment never covered such downstream reallocation costs and economic effects and did not motivate why it neglected them. Obviously, for commercial regulations such as the DSA, the main costs will not be the direct compliance burden, but the dynamic and downstream economic effects spurred by their implementation and how it changes business models and the behaviour of users. This is because this regulation will prompt firms and markets to change their current and future behaviour.[9] These dynamic changes are likely to define the most important effects on EU businesses and the economy at large. Examples of these economic and business costs, as well as trade costs may include, but are not limited, to the following aspects.

[8] Administrative costs are estimated in the Impact Assessment, but they are only covered partially and selectively.

[9] Fredrik Erixon et al. (2022) "After the DMA, the DSA and the New AI regulation: Mapping the Economic Consequences of and Responses to New Digital Regulations in Europe". ECIPE.

Economic and business costs

The EU Commission has argued that the DSA intends to address four problems in the functioning of digital services in Europe:[10] the fragmentation of the digital landscape, competitiveness, the risks for the online safety of citizens, and the information asymmetries and lack of monitoring. Addressing each of these four umbrella problems would result in differentiated economic effects, some of which may actually be positive and contribute to drive growth. However, some observers, like the Regulatory Scrutiny Board, are sceptical to what extent the implementation of the regulation would meet its objectives.[11]

Take the case of the fragmentation of the Single Market digital landscape. Since the implementation of the E-Commerce Directive in 2000, the growth of digital transactions has resulted in welfare gains both for EU businesses and consumers. Over the past 20 years e-commerce transactions contributed to an increase between 0.3 to 1.7 % in GDP per year for the EU.[12] Moreover, the digital environment has not only grown exponentially but also evolved to create new opportunities for business models. In response to these changing dynamics, Member States had to adapt by implementing different approaches to their legal frameworks. One consequence of these approaches has been the fragmentation of the business environment hampering the scale benefits of the single market. In other words, a reduction in fragmentation will drive benefits for platforms and their users. This effect of the DSA generates economic gains.

However, there can also be market exclusion effects as the regulatory barriers of the market go up. While there is a stated ambition on the part of the EU to generate better opportunities for online growth for SMEs there is a risk that the new regulatory demands in the DSA and other regulations will create new access barriers, raising the costs for businesses to engage in contracts on platforms, disproportionally affecting SMEs and small retailers.[13] Although the Commission anticipates a "one-time" upfront cost in its Impact Assessment, it is highly likely that the adoption of the DSA may result in larger impacts beyond the projected costs. After all, the DSA intends to prompt firms and markets to change their current and future behaviour, and it seems obvious that such change will have an impact.[14]

Furthermore, it remains to be seen *how* the DSA will contribute to reduce fragmentation in the EU market for digital services. While there is some harmonisation in the DSA, it also creates discretion for Member States. The implementation will effectively be achieved nationally. Add to that remaining differences in what is legal and illegal in each Member State in the area of information, which the DSA does not go into because there is no code for freedom of speech in the EU.

[10] European Parliamentary Research Service (2020) "Digital Service Act".

[11] European Commission (2020) Regulatory Scrutiny Board Opinion. Proposal for a Regulation of the European Parliament and the Council on a Single Market for Digital Services Act and amending Directive.

[12] European Parliamentary Research Service (2020) "Digital Service Act".

[13] Fredrik Erixon (2021) 'Too Big to Care' or 'Too Big to Share': The Digital Services Act and the Consequences of Reforming Intermediary Liability Rules. ECIPE.

[14] Fredrik Erixon et al. (2022) After the DMA, the DSA and the New AI regulation: Mapping the Economic Consequences of and Responses to New Digital Regulations in Europe. ECIPE.

Another issue that the DSA seeks to promote is competitiveness at the EU level. The Commission rightly identifies the need to minimise structural bottlenecks so that firms can grow and reap the benefits of the economies of scale offered by the Single Market. However, it does not address potential risks of dividing the regulation of platforms on the basis of size, and that the prospect of becoming fully covered by the DSA (the provisions that apply for VLOPs) may impede growth. In the Impact Assessment, the Commission states that "very large platforms represent the highest societal and economic risks because of their significant reach among citizens and traders in the EU."[15] While that observation is correct, the DSA's differentiation between large platforms and very large platforms may become an incentive for large EU platforms to remain at their current size rather than grow. One of the DSA's main aims is to create conditions for companies in the EU to scale their operations, but once they have surpassed a threshold, companies will be subject to a higher level of regulatory burden. Therefore, exposing VLOPs to tougher rules may in fact become a disincentive for large companies to grow and scale up further, especially if their platform has content that is difficult to subject to a legality check.[16]

A final issue concerns analysis of the traceability regime. There are clearly consumer protection gains with such a regime, and the Commission covers them in its proposal and the Impact Assessment. But there are also costs and those are not covered at all. For example, platforms themselves have raised concerns about the regime's impact on small businesses and individuals, especially by making services less user-friendly and user-centric and thus depressing the online market. In addition, it is critical to understand how platforms are expected to trace the traders. According to one analysis, the DSA appears to be more concerned with giving legal protection and clarity to intermediate service providers than with providing legal protection and certainty to customers who use their services.[17] On the latter point, the DSA is highly complex. The more complicated the data analysis becomes, the greater the challenges for e-enforcement.

In the final analysis, then, there are gains and costs of the DSA, but few of them have been subject to analysis in the Impact Assessment. There is a risk that the regulatory burden of the DSA could result in negative economic results. It is clear that the DSA champions a fair level playing field for businesses and a safe environment for users, but it is equally evident that the DSA could slow down Europe's pace of market and innovation change. There is little empirical evidence supporting the view that new liabilities to large companies and VLOPs will boost European digital companies and increase the rate of innovation within the EU.

[15] European Commission (2020) Impact Assessment for the Digital Services Act.

[16] Fredrik Erixon (2021) 'Too Big to Care' or 'Too Big to Share': The Digital Services Act and the Consequences of Reforming Intermediary Liability Rules. ECIPE.

[17] Caroline Cauffman and Catalina Goanta (2021) A New Order: The Digital Services Act and Consumer Protection. *European Journal of Risk Regulation*.

4. The Artificial Intelligence Act

4.1 What is the Artificial Intelligence Act?

The Artificial Intelligence Act (AIA) is a proposal from the European Commission that is currently subject to review and amendments in the Council and European Parliament. It will introduce a common regulatory framework for artificial intelligence in the EU. The final shape of the act remains unclear: both Member States and European Parliament Committees have tabled some profound changes to the original proposal. In fact, these changes even go to the heart of the definition of AI. For instance, while the Commission defined AI as a software that generates content, predictions, recommendations or decisions influencing the environments they interact with using a number of computer and statistical techniques,[18] the Council narrowed the definition to machine learning and logic and knowledge-based approaches. The European Parliament has also provided a new definition.

The AIA has two main goals. First, the AI Act will provide a set of common rules for the development and deployment of AI technology in the EU. Secondly, it will ensure that new AI systems respect fundamental rights and EU's values. In order to achieve these two goals, the act lays down rules that harmonise the use of AI in the EU and introduce an EU-wide framework for the enforcement of these new rules.

Even if the AI Act includes a broad range of techniques and affects all economic sectors with the exception of the military, not all sectors and AI applications will be regulated equally. The AI Act classifies AI systems into three risk-based categories: (i) unacceptable risk; (ii) high-risk; and (iii) limited and minimal risks. Each category is subject to different regulatory restrictions and obligations.

[18] Annex I of the proposed regulation lists these techniques which are: machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods, including deep learning; logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; statistical approaches, Bayesian estimation, search and optimization methods. However, the EU leaves the door open to include other techniques and approaches subject to the AI Act in the future.

The unacceptable risk category includes AI applications that are banned. For instance, AI systems that deploy subliminal techniques, exploit vulnerable groups, or are used for social scoring[19]. AI systems that fall under high-risks will be subject to extensive requirements. This category includes for example AI systems used as safety components of products falling under the EU health and safety harmonisation legislation[20] and AI systems that could infringe fundamental rights such as those deployed in biometric identification, management of critical infrastructure[21], education, human resources, law enforcement, migration, and democratic processes. In the Commission's proposal, AI systems that interact with humans like chatbots, deepfakes, and AI-powered emotion recognition systems are categorised as those with limited risks which will only require users to be informed that they are interacting with an AI system. For other AI applications there are no additional legal obligations[22]. Moreover, the inclusion of general purpose AI in the risk categories entail significant regulatory requirements.

4.2 Legal basis, subsidiarity, and proportionality

The legal basis for the AI Act is firmly placed within the core competences of the EU. The Commission argues that EU regulation is needed to provide safety and trust in AI, and to avoid the fragmentation of the internal market that may emerge if Member States start regulating the safety of AI on their own. To date, there is no specific regulation on AI approved internally by any single Member State yet. The need for harmonisation is emphasised by choosing a regulation rather than a directive to ensure an identical application of the new rules. There is also a legal motivation that builds on rights.

The proportionality of the regulation is grounded on its risk-based approach. In that regard, the need to respect the EU Charter of Fundamental Rights is called upon to justify the ban of certain AI applications which are deemed to infringe fundamental rights like non-discrimination, equality between women and men, and fair trial. For high-risk AI applications, the Commission argues that the new obligations are necessary to protect EU's fundamental rights and to minimise the risk of biased AI-assisted decisions.

[19] Real-time biometric identification used in public spaces also falls under this category except in a limited number of cases such as for targeted search for potential victims of crime, prevent a specific, substantial and imminent threat to the life or physical safety of persons or of a terrorist attack, and the detection of an individual suspected of a criminal offence referred to in the European Arrest Warrant.

[20] These products are machinery, toys, lifts, equipment and protective systems intended for use in potentially explosive atmospheres, radio equipment, pressure equipment, recreational craft equipment, cableway installations, appliances burning gaseous fuels, medical devices, and in vitro diagnostic medical devices.

[21] Critical infrastructure includes: the management and operation of road traffic and the supply of water, gas, heating and electricity.

[22] The AI Act, however, includes a code of conduct to encourage providers of non-high-risk AI systems to voluntarily apply the mandatory requirements for high-risk AI systems.

4.3 How does it work?

The most significant and novel obligations of the AI Act are those applicable to AI systems falling into the high-risks category. For these AI systems, the regulation includes a substantial number of new obligations. Providers of high-risk AI systems will, for instance, have to:

- Establish and maintain a risk management system.
- Ensure that training, validation, and the testing of datasets is subject to appropriate data governance and management practices.
- Publish and update technical documentation of a high-risk AI system before it is placed on the market or put into service.
- Incorporate logging capabilities to ensure a level of traceability of the AI system's functioning throughout its lifecycle.
- Guarantee a certain level of transparency and provide users with relevant information (for example the characteristics, capabilities, and limitations of performance of the high-risk AI system).
- Put in place measures to guarantee human oversight and ensure high-risk AI systems can be overseen by natural persons during the period in which they are in use.
- Design and develop systems in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity.

These obligations may seem straightforward, but they are surrounded by some technical, and sometimes conceptual, uncertainties when it comes to implementation. As an emerging technology with multiple applications, there is a degree of fluidity and diversity in the roles and responsibilities across firms forming the AI ecosystem. In the AI market, for instance, there is not a clear-cut distinction between "providers" and "users". AI systems may be developed entirely by one company or encompass AI tools purchased from multiple firms and patched together by another entity.

A similar argument can be made with respect to the data that feeds AI systems. The requirements on training, validation, and testing of data do not consider that these tasks may be done by different companies which complicates the assignment of responsibilities weaved into the regulation. In reality, companies have already put in place quality management systems and undertake due diligence when buying AI tools, systems and datasets. As the AI market develops and matures, this process is bound to continue organically. However, these new obligations risk spoiling these developments and instead solidify a way of working that is not necessarily what best suits market actors or the stated objectives.

Under the AI Act, to demonstrate that AI applications are compliant with the new obligations, firms will have to undergo conformity assessment; take action if the AI system is not in conformity; inform the public authorities of the corrective actions; and affix the CE marking to their high-risk AI system to indicate conformity.

The type of conformity assessment that AI systems will have to undergo varies across industries. AI systems used for biometric identification will require a conformity assessment by a notified body, which is an organisation approved by EU Member States to perform third-party conformity assessment.[23] The conformity of high-risk AI systems which are safety components of products covered by existing product safety legislation will follow the current procedures, which depending on the industry, may require third-party conformity assessment.[24] For all the other high-risks AI systems, the AI Act requires self-certification.[25] However, if an already approved AI system changes, either because of a technical improvement or a substantial modification of its behaviour due to learning, a new conformity assessment will be required.

This is important for AI because its ability to learn means that AI systems change endogenously, which brings questions with regards to when and how many times companies must prove conformity. The obvious risk is that multiple conformity assessments will carry costs for companies, particularly for SMEs and for industries where third-party conformity assessment is required. Moreover, many AI systems are highly customised products, often business-to-business, so compliance with the AI Act will become a significant fixed cost in the development of new AI systems, making them not just more expensive but also slowing down time to market.

A newly established European Artificial Intelligence Board will oversee the implementation of these new rules. The Board is composed of representatives from the Member States and the Commission. Member States will need to designate a national authority to supervise the implementation of the regulation while the European Data Protection Supervisor will act as the competent authority at the EU level. The EU will be in charge of establishing an EU-wide database in which providers of stand-alone high-risk AI systems will need to register their systems before placing them on the market or putting them into service. Ex-post enforcement of the AI Act will be done by national market surveillance authorities, which will have the power to intervene if AI systems generate unexpected risks[26]. In case of non-compliance, Member States will have the power to impose hefty penalties of up to €30 million or 6 % of a company's total worldwide annual turnover.

[23] A notified body is an organisation approved to assess the conformity of particular products before being placed on the market. The European Commission publishes a list of such notified bodies. European Commission, DG Grow (2019), NANDO.

[24] Third-party conformity assessment is performed by an independent entity, which is neither the producer, nor the user of the product.

[25] Self-certification, also known as first-party conformity assessment, allows the manufacturer or supplier of the product to carry out their own processes to declare that a product is safe. A formal document may be required, in the EU known as Supplier's Declaration of Conformity (SDoC).

[26] Market surveillance authorities will have the right to access the source code of an AI system which could put at risk trade secrets and intellectual property rights.

4.4 The potential impact of the regulation

Obviously, the AI Act will bring benefits. The new regulatory framework and the obligations on high-risk AI will increase trust on AI, can put European users more at ease when coming across AI technology. Ultimately, more trust in AI systems will contribute to a higher take-up of this technology. Moreover, similar to the Internet in the early 1990s, trust in AI is likely to increase over time as the sector matures. Many AI applications in analytics or supply chain management are also deployed within companies and therefore final consumers will not interact with these applications.

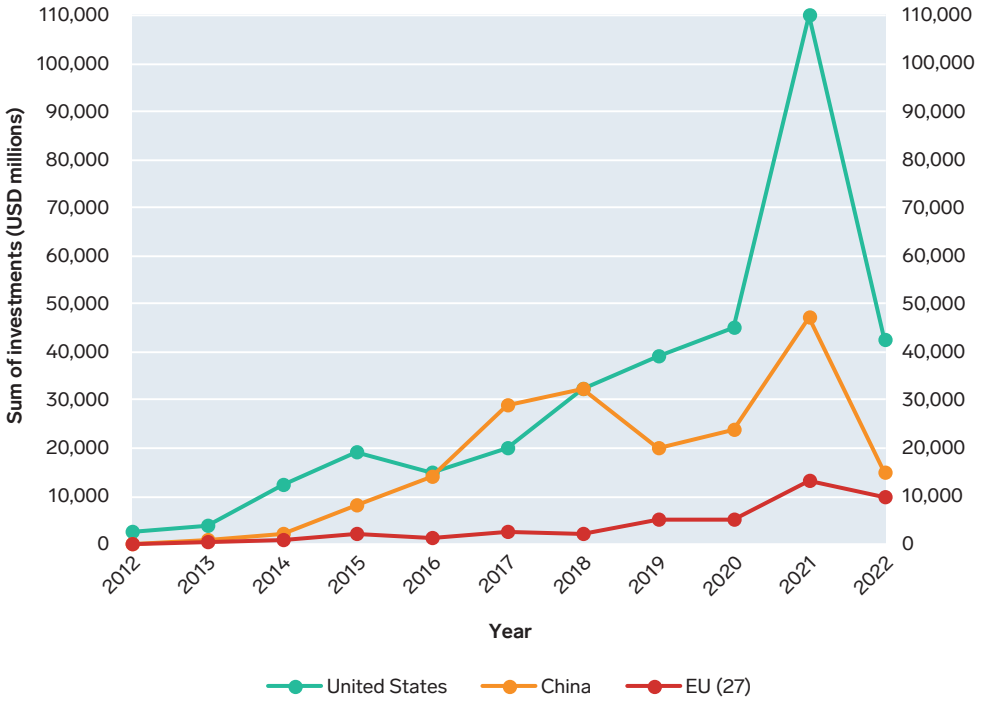
Furthermore, the Commission is also correct to say that the avoidance of fragmentation will lead to a better market in Europe. If the AI regulation can be shaped in a way (through objectives, concepts, and provisions) that makes it possible for standardisation bodies to develop simpler and effective standards, the regulation can generate benefits through a commoditised and standardised AI supply chain.

However, there are also costs associated with the regulation, and most of those are strangely absent from the Commission's analysis. The AI Act is a regulation of an emergent technology and, given the nascent identity of the AI applications market, may have a strong effect on the competitive position of the EU. While the AI sector in the EU has grown rapidly over the last years (in 2021, €11 billion of venture capital investments were made in AI compared to only €0.6 billion in 2016) the EU is at risk of falling behind other leading economies. AI investment spending at the Member State level in absolute terms has been the highest for large countries like France and Germany, while in per capita terms, the Nordic countries and Ireland come on top.[27] Despite these numbers, the EU is still far behind the US and China in terms of growth in the AI sector. As can be seen in Figure 4.1, venture capital investment in AI in the US in 2021 was €92 billion and €40 billion for China. In terms of number of AI start-ups, however, the EU was ahead of China (2,100 AI start-ups in the EU compared to 800 AI start-ups in China) in 2020, but still behind the US (4,800 AI start-ups).[28] This alone should motivate a rigorous analysis of the comparative economic effects of the AI Act. However, such an analysis was not done in the Impact Assessment.

[27] Karen Fullerton (2021) New AI Watch report: 2020 EU AI investments, European AI Alliance, European Commission.

[28] Mia Hoffmann and Laura Nurski (2021) The triple constraint on artificial-intelligence advancement in Europe. Bruegel.

Figure 4.1: Venture Capital investments in AI by country (2012–2022)



Source: OECD.AI (2022), visualisations powered by JSI using data from Preqin, accessed on 18/12/2022, www.oecd.ai

The Commission estimates that the new requirements described in the previous section will bring compliance and administrative costs in the order of €100 to €500 million.[29] These costs were calculated based on estimates of the amount of time that it will take for firms to comply with the new obligations. The time allocated to activities such as procuring data, filling forms or correcting was transformed into total costs using estimates on the number of companies affected by these new obligations and the respective wages of those professionals having to carry them out. This practice – based on the Standard Cost Model – is relatively common to produce a ballpark figure that informs policymakers about the average potential cost of new regulatory requirements. However, scaling up these results to produce cost figures for the EU is misleading. For example, in its impact assessment, the EU assumes that it will take a firm three minutes to familiarise itself with the obligations of the AI Act. While this may be true for some companies in Germany,[30] it will not be the case for many other companies across all EU Member States. In fact, it is most likely very, very far off the peg.

Yet, despite the efforts made in the calculations of the administrative costs, these will not be the most important economic impact of the AI Act. The EU Impact Assessment measures static costs such as administrative and compliance costs but it dismisses dynamic costs which arise as part of lower investment and innovation. It is very likely

[29] These estimates assume that only between 5 and 15 % of AI systems will belong to the high-risk category and as a result will have to comply with the most stringent requirements of the AI Act.

[30] Estimates on the costs of carrying out each activity were based on the German Normenkontrollrat.

that these dynamic and reallocation costs will be relevant. The AI Act regulates the way the AI market works, imposing requirements on companies across the whole AI supply chain which has direct effects on the way companies and professionals work, invest, and innovate. Moreover, as economic uncertainty in general is rising, the lack of clarity in some provisions of the AI Act described previously, i.e., doubts about which companies will have to comply with the new obligations and the frequency of the conformity assessments, is likely to delay and potentially deter the development of the AI industry in Europe.

Another economic risk associated with the implementation of the AI Act relates to its effect on the market structure of AI in Europe. A highly regulated and standardised AI market with higher conformity costs that bring higher overhead costs and uncertainties, may lead to larger companies cutting intermediate service suppliers – many of them SMEs – and investing in in-house solutions that lower the burden of the regulatory requirements set in the AI Act. In other words, the provisions within the AI Act risk shaping the market in a particular way, handing over the development and deployment of AI technology to the most prominent players while pushing SMEs out.

SMEs will be affected in a direct way, too. According to the European Digital SME Alliance, the compliance costs for SMEs that develop or deploy high-risk AI applications are estimated at around €7,000. Moreover, setting up a new quality management system is estimated to cost between €193,000 and €330,000, while the cost of obtaining third-party conformity assessment can be significantly higher. These additional costs will limit SME's ability to invest in the development and deployment of AI systems and subsequently hurt EU competitiveness. And even if the regulation includes exceptions for SMEs, these are unlikely to be used because most SMEs provide intermediate services to larger companies that will pass on these new obligations across their supply chains.

In the negative scenario, this effect will be contrary to the way the AI market is currently shaping up and will play against the EU's economic strength, which is based on SMEs. In 2020, 59 % of companies bought their AI systems from other companies while only 20 % developed them internally[31]. These figures point at an EU AI sector that relies on trade to acquire AI systems rather than on companies producing these systems in-house. However, since the new obligations of the AI Act will kick-in every time there is a transaction, the costs associated with these new obligations will likely push firms to undertake more AI-related activities within the firm and for the AI sector to become more vertically integrated. Obviously, the actual effect on the market structure remains to be seen, but it is noticeable that these types of economic effects were not included in the Impact Assessment.

Furthermore, there are likely to be cross-border effects of the AIA, and these effects are also uncovered in the Commission's assessment. The new rules of the AI Act not only apply to providers of AI systems established within the EU but also to those in a third country placing AI systems on the EU market or putting them into service in the EU. Underneath the philosophy of the AI Act, which stresses the need for a level-

[31] European Commission (2021) Impact Assessment of the Regulation on Artificial Intelligence, page 73.

playing field within the EU and between EU and non-EU companies, there is a strong desire to regulate AI globally. Given EU's market size and the technical complications and related costs of splitting a digital service or platform across jurisdictions, it is likely that the AI Act will have some extraterritorial impact. However, the notion that the EU will be able to unilaterally set rules that become worldwide standards, through the appeal of foreign companies to their governments, is doubtful.

First, other countries like Brazil, Canada, Japan, China, the UK or the US are also regulating AI or parts of it. Even though these countries may choose to follow a regulatory approach similar to the EU, their regulations will hardly be a "copy-and-paste" of the EU AI Act. Second, AI developers only need to follow the AI Act rules for AI services delivered to their EU customers. This is perhaps the most serious risk of the AI Act. By increasing the cost of developing and deploying AI in the EU, the regulation could act as a moat that separates the EU and the countries generating new AI systems, reducing the EU's innovation capacity. Many actual AI applications are bespoke and non-EU users would not benefit much from converging standards and regulatory behaviour to the regulatory norm established in the EU.

5. The Data Act

5.1 What is the Data Act?

In February 2022, the European Commission proposed a new legislation for the use of and access to data in the EU – the Data Act. The Data Act is part of the EU's Data Strategy whose ambition is to make more data available for commerce and society, while giving consumers and companies more control over what can be done with their data. With the Data Act, the Commission aims to achieve a multitude of policy objectives: ensuring fairness in Europe's digital single market, stimulate competition in data markets, open opportunities for data-driven innovation, and make data "more accessible for all".

More specifically – and in line with the Communication on a European data strategy – the Data Act aims to foster business-to-government (B2G) data sharing for the public interest and to support business-to-business (B2B) data sharing. It also aims to revise the EU's existing IP framework for databases to further enhance data access and use.

With the Data Act the Commission intends to address three key problems:

- Potential imbalances in negotiating power between data holders and those who wish to access the data they hold (which can lead to unfair data licence terms or a refusal to access to data).
- Inadequate private contracts for access to and use of non-personal data generated in industrial contexts (which could impede competition in certain markets and leave untapped the innovation potential presented by re-use of the data).
- Legal uncertainty surrounding the application of the Database Directive to machine-generated data and data generated in the context of IoT devices.

The European Commission claims that the Data Act will stimulate the creation of new, *innovative services* and more competitive prices for aftermarket services and repairs of connected objects. While assuming *non-rivalry in consumption*, the European Commission aims to target "legal, economic and technical issues that lead to data being underused".[32]

[32] European Commission (2022) Press Release. Data Act: Commission proposes measures for a fair and innovative data economy. 23 February.

5.2 Legal basis, subsidiarity, and proportionality

The legal basis of the Data Act is Article 114 of the TFEU, with ordinary legislative procedure and mechanisms for the EU to harmonise national application. It is argued by the European Commission that the Data Act will "further complete a single market for data, i.e. an area in which data from the public sector, businesses and citizens can be accessed and used in the best possible manner while respecting rights in relation to such data and investments made into their collection. Protection of confidential business data and trade secrets should also be safeguarded. Safeguarding the balanced outcome of the intervention will also be the objective for the review of the Database Directive. The initiative will allow the EU to benefit from the scale of the internal market, since data-driven products and services are often developed using data from different Member States, and later commercialised across the EU. Moreover, some Member States have taken legislative action to address the problems described above, in particular on the use of data by governments, whereas others have not. This can lead to legislative fragmentation in the internal market and different rules and practices across the EU and related costs by companies that would have to comply with different regimes."[33]

As concerns subsidiarity, the Commission claims that differences in national rules for data, cloud services and contractual rules are not conducive to competition and business activity in the Single Market. It is also argued that fairness of B2B contexts would be hard to achieve by different national rules that would lead to undesirable forum shopping. At the same time, it is explicitly stated that national polices could still be implemented if deemed necessary by EU government, e.g., in the realm of business-to-government data sharing.

Regarding proportionality, the Impact Assessment conducted by the European Commission concludes with the recommendation to implement "a limited set of legislative measures to facilitate the use of data, while strengthening legal certainty on how and by whom data can be used." It is argued that this would be the most proportionate set of policies "giving consumers and companies greater control over data, while limiting data holders' costs for making data more accessible and maintaining incentives to generate data."

[33] See, e.g. Inception Impact Assessment of the Data Act (including the review of the Directive 96/9/EC on the legal protection of databases).

5.3 How does it work?

To mitigate the problems identified by the Commission, the proposed Data Act includes several rules for access to and use of data in B2C, B2B and B2G contexts, such as a user control and a right to share user-generated data, a B2B fairness test, licensing on the basis of FRAND (fair, reasonable, and non-discriminatory) market rates and new rights for the public sector to access privately held data for public interest purposes. More specifically, for example:

- Article 4 provides that a data holder shall only use any non-personal data generated by the use of a product or related service on the basis of a contractual agreement with the user and prohibits the use of data "to derive insights about the economic situation, assets and production methods of or the use by the user that could undermine the commercial position of the user in the markets in which the user is active".
- Article 5 provides the right for a user to have the data generated through the use of a product or related service provided to a third party "without undue delay, free of charge to the user, of the same quality as is available to the data holder and, where applicable, continuously and in real-time".
- Article 5 (2) includes an exemption for core platform services of "gatekeepers" to be an eligible third-party data recipient under the Data Act data sharing regime.
- Article 8 requires that data provided to a data recipient must be under FRAND terms and in a transparent manner, with the obligation on the data holder to demonstrate that there has been no discrimination.
- Article 9 limits the compensation that a data holder can claim for making data available to that which is reasonable and, in the case of data provided to SMEs, the costs directly related to making the data available. In either case the data holder is required to explain the basis for the calculation.
- Article 14 obliges data holders to "make data available to a public sector body or to a Union institution, agency or body demonstrating an exceptional need to use the data requested." Article 15 provides a narrowing of the scope of "exceptional need" but leaves room for interpretation.
- Article 27 of the proposed Act includes several provisions that will affect the free exchange of non-personal data to jurisdictions outside the EU. Policymakers seem to be most concerned about commercially sensitive non-personal data such as trade secrets and intellectual property.

While the Data Act is a regulation with direct application, Member States will appoint competent authorities that will vouch for enforcement and deciding on violations and sanctions. It is assumed that several provisions will form the basis for a standards development, which will make the data market more standardised and open by design.

5.4 The potential impact of the regulation

Generally, the Data Act is a conglomerate of rules that cover very different aspects of data-related business. For example, businesses are expected to make technical and contractual arrangements on the basis of which data can be accessed and shared with users and third parties. Data processing services shall take technical, legal, and organisational measures to prevent international transfer or governmental access to non-personal data held in the Union where such transfer or access would create a conflict with Union law. Penalties apply in case of non-compliance.

As with all regulations, there are benefits and costs of the Data Act, and as with the other three digital regulations covered in this study, it is difficult to make a judgment of the size of the benefits and costs because they are inadequately covered in the Impact Assessment.[34] The Impact Assessment makes some extraordinary claims when it comes to the benefits. According to the underlying calculations, the Data Act will raise EU GDP by almost 2 % by 2028. If correct, this is a remarkably strong effect. On the cost side, the one-off implementation costs are estimated to be as small as 1 billion euro, with following annual costs in the region of 100 million euro. Again, if correct, these are remarkable results: a regulation, with significant impact on GDP, that is not associated with substantial implementation and administration burdens.

However, these estimates are most likely very far off the peg. There are certainly benefits that will emerge if there is a more seamless sharing and transfer of data in the EU. A standardised market will also generate benefits by making it easier to integrate data across sectors and firms. However, there are obvious negative effects that risk arising as well. Many of the provisions in the Data Act will have a direct impact on large data operations and thus be associated with costs.

The bottom line is that most provisions will create high compliance costs for businesses. Many of these rules will have an impact on the European data market and restrict the freedom to contract between, for example, a provider of cloud services and its customers. Obviously, the Data Act is designed to have an impact on especially a small group of big data operators, and to reduce their role in the non-personal data market. In addition, many provisions will have adverse dynamic impacts on investment and innovation in the EU, particularly less incentives to invest in data-driven innovation.

For businesses, the key provisions of the Data Act create *two major problems*:

- Type and scope of data for which sharing obligations apply: data holders face uncertainty over the types, aggregations and volumes of data that may have to be shared, the nature of third parties, e.g., potential competitors and governmental agencies, and when the data has to be shared with third parties.
- Compensation for data that is shared voluntarily or has to be shared with third parties: data holders face uncertainty over the amount of compensation, e.g., one-off or recurrent license fees, for data that is shared with third parties, both for voluntary and mandatory transactions.

[34] European Commission (2022) Study to Support an Impact Assessment on Enhancing the Use of Data in Europe.

In addition to the general data sharing framework of the proposed Data Act, the Commission may further use and possibly expand the provisions of data sharing obligations and compensation in sector-specific regulation in the future, for instance the European Health Data Regulation, adding legal uncertainty over the value of data and related business models on data holders operating in the EU.

Uncertainty over the actual scope of data sharing obligations and the amount of future compensation for complex datasets will impact on companies' decisions to invest in new technologies and business models that intensively rely on, generate or use, data. Some provisions in the Data Act effectively erode the protection of trade secrets and intellectual property rights, including databases (direct and intended effect), but also software, algorithms and ICT technologies (indirectly). There have been some proposed changes to them in the Council and the European Parliament, but the fundamental uncertainty remains. An expert study for the European Commission proposed in 2022 that it is warranted to wait and see how the data and data-sharing markets will develop before making far-reaching regulations.[35] If regulation takes place, much greater clarity must come on key concepts – and that includes how firms who share data should be compensated.

Due to substantial long-term investments which are accompanied by high commercial risks, legal uncertainty over the data exclusivity, co-ownership of data and the transactional value of data substantially reduce investment predictability and therefore can have a deterrent effect on investments in new technologies, business models and, generally, data-driven innovation in the EU. For example, the Data Act, could have a deterrent effect on innovative companies that aim to test and expand new data-driven business models in the EU, including Internet of Things (IoT) applications, in which many EU companies are already heavily invested.

These are risks, but the overall impact of the Data Act is difficult to assess. Its economic impacts will depend on the ultimate design and implementation of key provisions. The authors of the EU's own Impact Assessment have largely ignored these impacts. For example, a key provision is Article 5, which provides the right for a user to have the data generated through the use of a product or related service provided to a third party. Another key provision is Article 8, which requires that data provided to a data recipient must be under FRAND terms and in a transparent manner, with the obligation on the data holder to demonstrate that there has been no discrimination. These are very open provisions that, for example, can undermine the value of trade secrets and have a significant impact on the willingness to invest in generating data in the first place.

While the Commission does not substantiate its claim that Europe's businesses (and society at large) are suffering from shortages of or underinvestment in the generation of non-personal data (proclaimed market failure), it is also ignoring various risks involved with mandatory data sharing, including the erosion of incentives to create and share investment-intensive datasets, the disclosure of trade secrets, the

[35] European Commission (2022) Study on the legal protection of trade secrets in context of the data economy. European Innovation Council and EISMEA.

abuse by third parties and potential competitors, enforcement problems regarding the prevention and sanctioning of data theft, and implications for personal data safeguard measures (when anonymisation is challenging to execute).

With regard to FRAND obligations, the Commission largely ignored critical aspects of FRAND pricing, e.g. challenges in the market of standard-essential patents in communication technology industries, which is relatively small for data markets. For businesses in data markets, challenges include justifications for discriminatory pricing, administrative and procedural implications for data holders, and, potentially, an extremely high number of legal disputes between data holders and potential data recipients.

Another key provision is Article 5 (2), which includes an exemption for core platform services of "gatekeepers" to be an eligible third-party data recipient under the Data Act data sharing regime. The concept of gatekeeper, as set out in the Digital Markets Act, is complex, and may itself result in a wave of legal disputes over gatekeeper designation. At the same time, given the market structure of data-intensive industries in Europe and the success of US American companies in EU data markets, the EU should have investigated the reallocation effects of the Data Act. If one of the consequences is that data services are moved from efficient (gatekeeper) companies to less efficient data service providers, the negative effect on consumers and total value added is likely to be significant. Moreover, it could be prompt the US to retaliate against EU industries since the large (gatekeeper) data service providers are predominantly American.

Another example of an economic effect that motivates deeper analysis than has been provided in the reports for the Impact Assessment is Article 27, which includes several provisions that could severely hamper the free exchange of non-personal data to jurisdictions outside the EU. The Commission seems to be most concerned about commercially sensitive non-personal data such as trade secrets and intellectual property. It is assumed that international transfers of non-personal data require an equal regulatory regime to what exists for personal data under the GDPR. Accordingly, Chapter VII of the proposed Data Act draws from GDPR important concepts such as data portability and conditions for international data transfers. Article 27 provides specific safeguards, by way of providers having to take all reasonable technical, legal, and organisational measures to prevent unlawful third-party access that conflicts with competing obligations to protect such data under EU law, unless strict conditions are met. The application of these provisions in the Data Act raises many questions. One risk is obviously that a company in Europe, that has invested in data and built a model of protection that includes IP and trade secrets, may not be able to use data services abroad.

In sum, the economic effects could be substantially different from the 2 % GDP expansion proposed in the Impact Assessment. A study by Frontier Economics on the economic impacts of restrictions to the cross-border flow of non-personal data finds that new regulations, which entails EU businesses having to assess the laws and practices of non-EU countries before they share non-personal, commercially sensitive data, would cause 40 % of surveyed businesses to stop their cross-border flows of such data. This is very significant. Large EU businesses and multinational EU corporations expect costs equivalent to on average 4 % of their annual global revenues.

The impact is expected to be larger for R&D-intensive companies that share data for innovation purposes. It is highlighted that such regulations would act as a tax on R&D, innovation, and business scale-up in Europe as these costs are non-recuperable costs, diverting EU businesses' resources away from productive investments in future capacities and capabilities.[36]

Overall, Frontier Economics estimates that the cost of new restrictions to the cross-border flow of non-personal data to multinational enterprises and scaleups would be around EUR 79 billion per year, of which 20 billion would be from impact on scaleups and 60 billion from impact on other MNEs. This is around 0.6 % of EU GDP. It is highlighted that European SMEs account for a minority of the overall impact, around 40 % (EUR 26 billion). This is because large enterprises are more likely than SMEs to have an international presence and therefore to share data across borders.

Finally, Article 27.3 empowers the European Commission to develop guidelines, consistent with the recommendations of the European Data Innovation, for transfer risk assessments, which could rely on key cybersecurity requirements. In this context, the EU Agency for Network and Information Security (ENISA) is proposing a far-reaching Cybersecurity Certification Regime for Cloud Services (EUCS) provided in the European Union. ENISA is following a request from the European Commission, which is considering mandatory cybersecurity certification in several EU policies targeting providers of ICT products and services in the EU, including the Data Act. According to the latest draft of the EUCS, its provision (especially the proposed "immunity requirements in EU cloud certification), would exclude many legitimate EU and foreign suppliers from providing secure cloud services to customers in the EU.[37]

[36] Frontier Economics (2022) Beyond Personal Data: The Cost of Data Flow Restrictions to EU Companies. 17 February.

[37] ENISA (2021). Cloud Certification Scheme: Building Trusted Cloud Services Across Europe. Press release.

6. Analysis of the impact on markets and trade policy

The previous chapters have presented the objectives, concepts, and operations of the four digital regulations covered in this report. We have also reviewed the quality of the regulatory process, especially the Impact Assessments, with the view of getting an understanding of the extent to which the legislator has a clear understanding of costs and benefits, and what trade-offs that each regulations presents.

In this chapter, we will deepen the analysis of the market and trade effects of new digital regulation and especially consider the consequences for EU trade policy. The first part will outline important economic concepts for the economic analysis of digital regulations, and point to where there, generally, are missing elements in the Impact Assessments. The second part will review if there are reasons to believe that elements of the new digital regulations will violate the EU's international obligations. Finally, the third part will consider risks of retaliation.

6.1 Market and trade analysis

The economic impacts of the four regulations were appraised in their respective Impact Assessments. However, in its respective analyses of the various regulations, the European Commission only presented a limited range of impacts. Most of the attention was devoted to calculating static costs such as administrative and compliance cost for firms and governments derived from the new obligations. As a result, dynamic costs such as the effect of the regulations on trade, investment, or innovation were left out. These weaknesses were reflected in the reports of the EU's Regulatory Scrutiny Board (RSB) which marked several of the preliminary Impact Assessments with a negative opinion.

The four digital regulations share a number of economic effects. The new obligations will influence trust, market utility, scope, scale, supply chains, and the degree of integration and fragmentation in the market. Inevitably, these economic effects will impact cross-border exchange in the form of trade but also investments and exchange of knowledge. These cross-border effects hardly feature in the Commission's assessments, but they probably matter a lot. The digital economy is global, and these regulations have direct effects on market structures and costs that will inevitably impact the way European firms trade and relate with the rest of the world.

In this section, the economic effects of digital regulations are used as a tool to uncover the broader market and cross-border effects. The four digital regulations impact the same kind of trade flows, namely trade of data and IT services, restricting the EU's ability to buy and sell digital services abroad. The following section discusses which countries are likely to be most affected by these changes and in which sectors, how these effects will lead to a reconfiguration of the EU digital economy and ecology, and its reliance on other countries with respect to the production of digital services.

The starting point for this analysis is the economic effects brought by the four regulations. Each section starts with the definition of the economic effect. Then it describes how these economic effects manifest in the digital regulations and how they translate into trade effects. Lastly, we consider the current flows of trade that all four regulations will impact. A forthcoming paper will estimate the quantitative effects on trade from the regulations covered in this study; this chapter considers only qualitative and conceptual aspects.

Trust

One of the key objectives pursued by these regulations is to build trust in digital services and technologies. The underlying assumption behind this search for higher consumer trust is that it will lead to higher demand for digital services and technologies, and therefore technological diffusion and economic prosperity. While this is a logical argument with real implications in some specific regulations, there is hardly any evidence in the EU analysis as to how much an increase in trust will result in higher take-up of digital services and technologies. It can be argued that, at the beginning, trust in new technologies is always low and rises as consumers get accustomed to it and the market matures. An example of this organic growth in consumer trust can be found in the development of the Internet.

Building trust is one of the main goals of the Artificial Intelligence (AI) Act and, to a degree, of the Digital Services Act (DSA). Yet, an important difference between the AI Act and the DSA is that the AI Act will regulate AI in the EU when this industry is at its inception. Therefore, it could be argued that while the AI Act will increase trust in AI systems which will drive up demand of EU and non-EU AI products, it is less likely that the DSA will generate additional demand for internet services since they are already mature services that people in general are familiar with. While there is scepticism among users of some Internet services about how much information they give away to platforms, it is unlikely that this is going to change as a result of the DSA. As social media steps into the metaverse or develops other forms of immersive virtual "worlds", it can be argued that trust can be increased by regulation.

The increase in demand for AI systems will likely lead to an increase in EU imports and domestic production of AI and inputs for the AI value chain. All else equal, EU imports are likely to come from the US since this economy is the leader in terms of investment (€92 billion in venture capital investment compared to €11 billion in the EU) and number of start-ups (4,800 start-ups compared to 2,100 in the EU). However, the AI Act can impede on that import if the EU and the US markets diverge regulatory.

Market Utility

Market utility is defined as the ability of the regulation to impact the utility that consumers received from using a particular service. This economic effect is clearly visible in the Digital Markets Act (DMA), the AI Act and the Data Act. For example, the provisions in Article 5 of the DMA restrict the ability of gatekeepers to offer certain digital services. By cutting off the connections between services, which seems to be one of the essential effects on platform services in the DMA, the Act may put more weight on a target for market concentration than on consumer welfare. This is because the economic features that restrict competition – those arising from network effects and two-sided markets – are exactly the features that increase the utility of the services offered by the gatekeeper. In these markets, lower competition is the downside of higher utility.

Similarly, if the Data Act will have the effect of reducing the role of large (gatekeeping) cloud providers in Europe's data sharing market, the market utility of cloud services is likely to go down as well. In the AI Act, a similar effect could emerge if general purpose AI system are subject to significant restrictions. It may have the effect of lowering the market utility of an AI application.

Scope

Limiting the services that the gatekeeper can offer lowers their market scope and the ability to have deep integration in a market. One of the main assumptions in the Commission's Impact Assessment of the DMA is that those services that will no longer be provided by the gatekeepers will be provided by someone else, at the same cost and quality. Similarly, the underlying economic philosophy in the Data Act is that the data-sharing exclusions of large and foreign cloud providers will have no impact on service quality: European providers will just substitute the American providers.

These are bold assumptions. First, the services no longer provided by foreign companies may not be provided by European companies at the same quality. If, for instance, AWS, Google, IBM, and Microsoft cannot participate in some data service operations, this would have huge consequences on market structure and the quality of services. Second, other EU or non-EU companies may be able to provide these services but only at a higher cost. Moreover, limitation on the provision of services by gatekeepers will not impact all EU Member States equally. For small EU Member States, it will be more difficult to find alternatives than for larger EU Member States.[38]

The issue of scope also relates to the dynamic effects on innovation. While it remains an open question whether some companies will be able to substitute the services that are no longer provided by gatekeepers, it seems likely that gatekeepers will invest less on services that they cannot provide. Part of the missing investments will be in the update of the current services, but other investment will be on the Research and Development (R&D) spending for new services.

[38] Fredrik Erixon et al. (2022) After the DMA, the DSA, and the new AI regulation: Mapping the economic consequences of and responses to new digital regulations in Europe. ECIPE.

The DMA and the DSA may have positive effects on innovation due to their interoperability provisions, which would help European start-ups that struggle with scaling up. At the same time, the threshold effects of the regulation also lower the incentives for digital firms to scale up above a certain point. Scope (additional services and innovation) and scale are related factors in the digital economy to the significant fixed costs associated with providing digital services.

Scale

The key scale effect of the digital market is that bigger scale reduces the variable cost of a service. From data centres to brand recognition, digital services require significant fixed costs while variable costs are much smaller and could be next to zero in the margin. This economic feature – particularly relevant for digital services – is important when thinking about the trade effects of digital regulation. An example are data storage costs, obviously driving huge energy demand. Services that operate at scale are more efficient and can reduce the cost of storing data.

As it is the case of the DMA, but also the AI and the Data Act where the EU market is being segregated from the rest of the world, if companies need to disentangle their offer of digital services, it is likely that they will end up with a fewer number of users. As a consequence, the cost per user – which is mostly fixed costs – will increase, making the digital services and technologies more expensive and reducing the volume that will be traded.

Most of the companies that will be restricted in the Data Act and the DMA because they are gatekeepers represents a big part of the EU imports of computer and information services from the US These companies have invested heavily in the production of digital services, which due to the significant fixed costs, will not be easy for EU companies to match. While the restrictions in these regulations may benefit domestic EU firms in IT, other sectors will suffer as a result of higher costs. This is particularly relevant for the sectors undergoing a digital transformation, some of them where the EU shows a high level of competitiveness. For instance, the production of autonomous vehicles requires a tremendous amount of data collection, storage and processing that are offered mainly by US cloud service providers.[39] The commercial ties between the US and the EU helps accelerate the digitalisation of the automotive industry, which is the biggest R&D spender in the EU[40], by leveraging the high fixed costs of R&D investments.

Integration and fragmentation

Some of the new regulations will help to drive growth in the EU data market and AI because they will establish new standards that will commoditise and standardise specific services. Moreover, the Data Act can help to drive growth for SMEs by facilitating greater participation by them in the data market. These are important integration effects that lead to market inclusion and reduced costs for professionalising the supply and value chain in these markets.

[39] Companies such as Volkswagen and BMW are investing massively in digitalisation and rely on US cloud service providers.

[40] McKinsey Global Institute (2019) Innovation in Europe. Figure 7.

There are also fragmentation effects. Many of these regulations are not discriminatory by definition since they impose the same obligations to EU and non-EU companies selling their products in the EU. However, by imposing costs on digital services and technologies in the EU, these regulations drive a wedge between EU and non-EU prices of digital products.

For example, the European Commission estimates that the new requirements of the AI Act will impose costs in the order of €100 and €500 million. At the individual firm level, the European Digital SME Alliance estimates that setting up a quality management system to comply with the AI Act could cost between €193,000 and €330,000, while the cost of obtaining third-party conformity assessment can be significantly higher. These costs will particularly be damaging for SMEs. And while the AI Act includes exceptions for SMEs, these are unlikely to be used because most SMEs provide intermediate services to larger companies that will pass these new obligations across their supply chains.

Given the prescriptiveness of all new digital regulations and high degree of compliance due to the hefty fines,[41] these regulations will impact trade and investment decisions. By increasing the cost of digital services in the EU, the regulations act as a moat separating the EU and the countries where the EU buys and sells digital services. For instance, the AI Act will lead to higher conformity costs for AI systems sold in the EU, the DMA lowers the incentives for gatekeepers to provide new services to the EU market, and the Data Act increases the costs of storing data outside the EU. Overall, these digital regulations act like an import tariff, changing the relative prices between intra and extra-EU digital services, hampering EU competitiveness.

The underlying assumption in some policymakers' minds seems to be that the EU is the midget of the digital economy. Therefore, it is better for the EU to protect its market and consumers rather than promoting openness and the EU's digital trade. The statistics, however, tell a different story. The EU is not only the largest exporter and importer of telecom, computer, and information services but it has a significant trade surplus in computer and information services.[42]

Supply chains

Higher prices for digital services will hamper EU companies producing digital services for the EU and non-EU market. Imposing specific conditions for digital services and technologies sold in the EU puts a spoke in the wheels of EU firms that are part of global supply chains of the digital economy. Moreover, higher cost, lower availability and delays of time to market for digital services and technologies[43] put all EU firms at a disadvantage when competing with non-EU companies in third markets. As an example, losing on the quality of online search, cloud computing, and advertising through social network services due to new regulations will disadvantage European firms.

[41] In case of non-compliance, Member States will have the power to impose penalties of up to €30 million or 6 % of a company's total worldwide annual turnover.

[42] Anecdotal evidence in the Fintech and Enterprise Software sector show that the European tech ecosystem has consistently produced breakout companies.

[43] Rebecca Janssen et al. (2022) GDPR and the lost generation of innovate apps. NBER Working Paper No. 30028.

The multiple limitations of the digital regulations are a hammer on the EU digital economy, cutting EU companies from the latest digital technologies and obstructing collaboration with non-EU companies at the frontier of their respective digital services. Many EU companies active in the digital economy are providers and users of digital services. Digital regulations impose costs on the services that these companies can supply (e.g., the AI Act) and the inputs – services, data, and data storage – that these companies need to deliver their services (e.g., DMA, AI Act and the Data Act). In addition, the uncertainties in the implementation of these regulations will impact firms trading in digital services. For instance, there is considerable uncertainty as to when and how many times companies have to prove conformity in the AI Act or as to how exclusivity rights will be applied, and therefore IP protected, in the data sharing provisions of the Data Act.

The EU relies on its market size – which is significant – as a magnet for non-EU companies to follow EU regulation. And while it is true that, given EU's market size and the technical complications and related costs of splitting digital services or platform across jurisdictions, it is likely that the digital regulations will have some extra-territorial impact, the notion that the EU will be able to unilaterally set the digital rules that become worldwide standards is doubtful. On other hand, these regulations may lead to non-EU companies making investments in digital capabilities within the EU. For instance, Amazon, Google, and Microsoft have made significant investment in data centres within the EU. While these investments may lead to higher economic activity in the short run, they may also lead to higher prices, particularly as a result of the effect on scale described before.

In any case, all foreign firms wanting to sell their digital products in the EU will be impacted by these new digital regulations. However, given the EU's economic integration with the US and their leading role in the development and deployment of digital services and technologies, EU-US digital trade will be most impacted by these digital regulations. This is particularly important to observe because of the supply chain specialisation emerging at both sides of the Atlantic, which shows a considerable level of economic integration.[44]

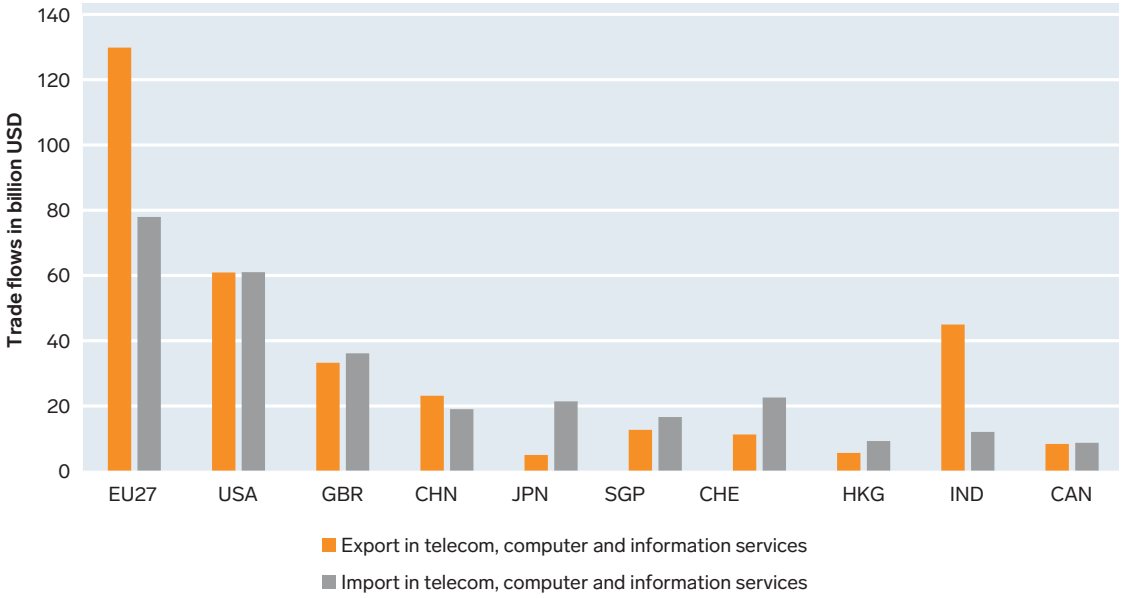
In order to maintain its trade surpluses in computer and information services, the EU relies on the US for digital technology. The statistics show that the EU is a net buyer of IP and R&D services, and the US is Europe's main source of this knowledge. At the same time, the trade figures suggest that, within the supply chains of digital services, the EU has significant strengths in final digital services. The risk carried by these digital regulations is that the EU will stop having access to the most advanced digital technology produced outside the EU, hurting EU's productivity growth in its digital and non-digital economy.

[44] For example, in 2021, US companies represented 39% of capital invested in EU start-ups in rounds larger than $20 million, while Asia represented 13 %. Moreover, A string of big-name US-based investors like Coatue, General Catalyst and Iconiq Capital have set up offices in the Europe in recent years.

EU Trade in digital services

Finally, let us look at EU trade in digital services. In 2019, the EU exported $131 billion of telecom, computer and information services, and was the largest exporter before the US, India, and the UK and imported $79 billion, making it the largest importer of these services before the US, the UK, and Switzerland. This is a significant position and trade surplus.

Figure 6.1: Exports and imports of telecom, computer and information services



Source: OECD

At a more disaggregated level, the EU also enjoys a trade surplus in digital services like computer services and information services.[45] In 2021, the EU exported €196.2 billion of computer services and imported €170.9 billion. More than one fifth (19 %) of EU exports and more than one-third (36 %) of EU imports of computer services went and came from the US. In information services, the EU exported €9.8 billion and imported €5.7 billion. In this case, the primary source of imports was the US (35 % of total imports) while for exports, the EU's main destination was the UK (35 % of total exports).[46]

Even though the EU has a trade surplus in digital services, it is a net importer of digital technology. For instance, in 2021, the EU paid €170.9 billion for the use of Intellectual Property (IP) while it received €98.3 billion and exported €46.8 billion on research and development services and imported €81.8 billion. In both cases as well as for EU exports (amount received for IP) and imports (amounts paid for IP), Europe's main partner was the US. In the case of IP, US. firms represented 74 %

[45] Full name: Information services other than news agency related services

[46] Eurostat data on international trade in services, https://ec.europa.eu/eurostat/databrowser/bookmark/8c9ea592-670f-4693-b955-7b7c2ed5a8bd?lang=en

of the amount paid and 44 % of the amount received for IP. In relation to research and development services, the US market was 43 % of EU total exports and 42 % of EU total imports.

6.2 Trade policy analysis

In this section we will take a closer look at international trade agreements that the EU has signed and how the covered digital regulations relate to them. The four regulations included in this analysis have consequences for Europe's trade – and other cross-border flows – but they *could* also impact on different obligations that the EU has signed up for in international agreements. It is generally difficult to say to what extent there are consequences on existing trade obligations because the application of these regulations is sometimes unclear: it is difficult to say, for instance, how various gatekeepers will be impacted by the obligations and restrictions in the Data Act and the Digital Markets Act.

Uncertainty about the legality of different regulations is exacerbated by the fact that digital regulations are an evolving field of regulation and that there is precious little jurisprudence from the WTO relating to digital regulation – or regulations that lead to "unlike" treatment of traders in digital services that are covered by bindings in the schedules in the General Agreement on Trade in Services (GATS). There are GATS cases that relate to the digital economy and especially the electronic transmission of services – e.g. electronic payment services – but they are not specific to the digital regulations discussed in this study.

Moreover, there has not been any official analysis of these international trade-policy effects by the European Commission. To the extent that trade-policy aspects are covered in the Impact Assessments of the four regulations, they mostly come in the form of non-analytical statements. Hence, as a first observation, it can be argued that the analysis provided in EU Impact Assessments of the different regulations on their compliance with the EU's international obligations is inadequate.

The Impact Assessment of the Digital Services Act briefly states that the regulation is in full compliance with international trade rules by outlining that the EU "has a wide range of trade commitments in sectors covering digital services. This initiative will be in full compliance with the EU's international obligations, notably in the multilateral agreements in the WTO and in its regional trade agreements."[47]

Regarding the different policy options assessed by the EU impact assessment of the Digital Markets Act, it mentions that all options "are designed in such a way as to target any gatekeeper platform in an objective and non-discriminatory manner (…). The objective scoping criteria applicable to all options target EU presence and do not take into account the location of the corporate headquarters of the company in question. In doing so, the options would be future-proof and consistent with

[47] European Commission (2020) Impact Assessment for the Digital Services Act. SWD (2020) 348 final, page 6.

the EU's international obligations, including non-discrimination under the General Agreement on Tariffs and Trade and the WTO. The EU is a major market which will remain open for business but competition in the EU should remain fair and markets contestable."[48]

In contrast, the Impact Assessment of the Artificial Intelligence Act does not make direct reference to compliance of the regulation with the EU's international obligations. Similarly, the impact assessment of the Data Act does not include direct reference to the compliance of the regulation with international rules. However, it includes a general statement (and an annex providing an overview of relevant legal initiatives) which refers to the importance of international commitments. It says: "International data processing and storage as well as data transfers are governed by the GDPR, trade commitments under the WTO (GATS) and bilateral trade agreements, in particular on computers and related services."[49]

These analyses of WTO or other international legal contexts are insufficient. While these digital regulations *may* stand up in a legal review and a dispute, it is highly advisable that the EU pays far more attention to the consequences of these regulations on the trading rights of other countries. There are four good reasons for it.

First, the EU is a keen defender of the WTO and the international system of rules that manage global economic and commercial affairs. It is a system that has hugely benefit Europe and spurred international economic development. It has spent much more time and energy than the US and China to resolve problems holding the WTO back, and if the EU cannot demonstrate it takes the system and its obligations seriously, it should not expect others to do it either.

Second, the EU has a big trade surplus in digital services and has offensive economic interests to defend. A policy by the EU that reduces market access for trading partners may lead to reciprocal actions by the partners.

Third, the effects of all four regulations are concentrated to certain categories of services trade. While the regulations may differ in purpose and scope, it is by and large the same trade flows and the same traders that are affected. Hence, there is an accumulation of new regulations with combinatory and most likely, significant impacts on certain flows of trade.

Fourth, the geographic effects of these four regulations are also concentrated: they disproportionally affect the export of services from especially one country: the US (see the next section). Both concentration effects make it likely that the regulations will be challenged on grounds of the denial of trading rights. The EU could pre-empt frictions and disputes by providing a better legal analysis in its work to assess the impacts of its policies.

[48] European Commission (2020) Impact Assessment for the Digital Markets Act. SWD (2020) 363 final, page 86.

[49] European Commission (2022) Impact Assessment for the Data Act. SWD (2022) 34 final, page128.

There are three areas that need deeper legal analysis. First, the digital regulations covered in this study (and others, of course, like the EU Cybersecurity Certification Scheme for Cloud Services and the EU Cyber Resilience Act, which comes with direct forms of discrimination) may have consequences for services market access. In other words, the EU may have signed up to market access obligations that will be denied to some foreign firms as a consequence of the regulation. While there can be justified exemptions from market access bindings and the core principle of likeness, these exemptions would be conditional and must be motivated on the grounds stated in the GATS. Second, the regulations provide obligations on companies to reveal – and possibly share – certain aspects of their practices, and some of these practices may be protected by intellectual property rights and trade secrets. As the EU is signatory to several agreements with consequences for IPRs, there may be a conflict here. Third, and last, the regulations go into territories of competition policy and how competition policy can be used: international agreements have consequences also for such instruments.

Intellectual property

The core obligations for the protection of intellectual property rights in international trade are established in the TRIPS agreement in the WTO. This agreement includes a set of intellectual property rights such as patents and copyrights, and it establishes rules for the conduct of nations in matters of IPRs. Many of the core provisions in TRIPS are reflections of other international property rights agreements, which had been negotiated and agreed long before the advent of TRIPS. These international agreements also form the basis in several bilateral trade agreements that the EU has signed. Moreover, these bilateral trade agreements often have IPR provisions that go beyond TRIPS obligations and thus provide a somewhat stronger legal framework for IPR protection compared to TRIPS. Notably, the EU has been a keen proponent of extending the strength of IPRs in trade agreements.

These agreements on intellectual property rights are important for the digital economy and may have consequences for the legality of new digital regulations. Some of the regulations covered in this report have provisions that could relate to the rules on intellectual property and trade secrets of firms that are likely to be subject to the new regulatory obligations. For instance, the DMA ushers in new rights for third party business users to access data on a platform. While the legislator has made efforts to specify what data that the right relates to – an access and portability right for third-party business users for data generated by them and their end users on the platform – it is far from clear in practice what data that henceforth should solely be the product of the third-party user. Other regulations in Europe have made efforts to define certain data and specify certain data rights (e.g. the InfoSoc Directive, the Software Directive and the Public Sector Information Directive) but they incorporate an equal amount of uncertainty and have stopped short on using concepts and definitions that could infringe on intellectual property rights and trade secrets.

Further complication arises because of the complex nature of intangible and digital assets, and the role of data in generating assets. The reality of the modern intangible economy is that companies have a variety of different types of intangible assets that have different forms of legal protection. Jurisprudence on all these issues is rarely

clear, especially in an international context, and uncertainty has grown over data as it forms part of many of these assets. While data itself is not protected by IPRs, data can be generated by protected assets and be part of a trade secret. The structure used to organise data, such as a database, can be afforded intellectual property protection. Moreover, the actual operation of using and generating data by algorithms often lead to complex products and assets where the exact relations between data, the organisation of data, and their use and outcomes are hard to disentangle. With machine learning and the broader development of Artificial Intelligence, such legal complexities are growing – especially as such developments often include increasingly complex structures of firms sharing data. Notably, these complexities are also exacerbated by remaining uncertainties about the European patentability computer-implemented inventions, and differences between the legal situation in the EU (it is not an EU issue) and the US in this regard.

What new DMA provisions on third-party access to "their" data on a platform actually mean remains to be defined, but it is clear that there are risks that these definitions may be problematic for trade secrets as well as protected assets. Other digital regulations include provisions of similar or related nature, and – as in the case of the Digital Service Act – veer into issues about algorithmic transparency. The Data Act provides for far-reaching data access and portability rights but have similar problems of making clear what data and compilations of data that reasonably should be subject to these rights – or, indeed, exactly what third parties that should be afforded these rights and on what terms. The issue about data definition is something that the Regulatory Scrutiny Board complained about in its review of the Data Act and its Impact Assessment: it is and remains unclear but could, in an extensive interpretation, lead to very significant effects on firms that hold data and what they will be mandated to share. A text-based interpretation of the Data Act can give rise to far-reaching and mandatory access rights – and, in that case, it is easy to observe that there will be clear frictions with international rules on intellectual property protection and trade secrets.

All the specific examples and provisions above clearly relate to data, compilations of data and data generated by "technologies" that enjoy protection under rules of intellectual property rights. The TRIPS agreement – and other agreements that incorporate TRIPS – could have consequences on the legality of these measures, just as the EU's own intellectual property protection can impact on them, if the actual implementation of the regulations will be on the heavy-handed side. First, the TRIPS agreement makes clear that trade secrets and undisclosed information are assets that should be awarded intellectual property protection in countries that have signed it. Second, the TRIPS agreement has particular rules (Article 10) on the protection of "computer programmes and compilations of data" – including source and object codes – that by its selection or arrangement is an intellectual creation. In other words, computer software and datasets can be protected under copyrights. The origin of this rule was the non-specific coverage of computer programmes and data sets in the Berne and Paris Conventions, the main international copyright agreements. With the development and growth of computer and data-based business models in the 1980s, and its increasing importance for trade, the TRIPS agreement added a specification, and made it broad and encompassing, including the selection and arrangement of data compilations (e.g. databases).

In a parallel development, a group of 64 countries – including the EU – also developed a new international treaty on copyrights, the World Intellectual Property Organisation Copyright Treaty (WCT), to explicitly address issues related to copyrights in the digital economy. The WCT, which took effect in 2002, builds on the Berne and Paris Conventions and the TRIPS agreement. It uses the same language to define the coverage of data-based intellectual creations. It says that copyright protection should be given to "compilations of data and other material, in any form, which by reason of the selection or arrangement of their contents, constitute intellectual creations." It also includes an important distinction: "This protection does not extend to the data or the material itself and is without prejudice to any copyright subsisting in the data or material contained in the compilation".[50] Furthermore, the WCT also included certain rights for different holders of copyrights, including the right to distribution and the right to rental.

The TRIPS agreement does not come with general exemption rules which allow for substantial derogation. Possible exemptions exist but they are predominantly of administrative nature. Some bilateral trade agreements have more specified provisions on trade secrets (including possible derogations through new definitions of how a trade secret has been obtained) that are applicable to the above-mentioned provisions in the new digital regulations (e.g. the EU-Japan agreement). However, the TRIPS agreement remains the basis for these agreements.

A final legal analysis requires more information than available now about the application of the new provisions in, for instance, the DMA and the Data Act, and how they will impact on rights under the TRIPS agreement. However, it is obviously the case that there are friction points between some of the new provisions and international rules on the protection of intellectual property. One group of frictions relate to access and portability rights for third-party users. The Data Act in particular, but also the Digital Markets Act, will most likely have problems of providing exact definitions and distinctions of what constitutes data and who has the right to it, and how those rights relate to assets that are protected by trade secrets and copyrights. A third-party business user brings data to a platform that is directly created and compiled by the third party, but the use of a platform service or a platform algorithm creates data that is derivative and substantially a function of a protected intellectual property – including the data relating to the assets of other third-party business users.

Some of the provisions in these new digital regulations also have wider consequences and an extensive use of these new provisions to deny trade secret protection for certain exporters can establish precedence that can affect the rights of protection for EU firms in other countries. For instance, in December 2022 the EU filed a complaint to the WTO about alleged violations by China of protecting high-tech patent holders. Europe has routinely demonstrated disappointments with practices in other countries that are dismissive of issues related to trade secrets protection.

[50] WCT Article 5.

Competition policy

Concerns relating to international agreements in the field of competition policy are less clear than in the case of IPR protection. Competition policy is not subject to broad encompassing international agreements that confer rights to countries and that builds on the key principles of international trade – like likeness – that have direct application in a country's conduct of competition policy. There are international agreements of importance for state aid and state-owned enterprises, including a WTO agreement and OECD accords. In matters of anti-trust, especially measures for regulating mergers and acquisitions and the denial of business freedom rights on the basis of anti-trust motivations, international agreements are less prevalent and significant.

The EU basis for international cooperation in this area are dedicated bilateral agreements and protocols on competition policy, and chapters on competition policy included in other bilateral agreements. Being a big region for economic activity and companies with international reach, the EU has an extensive network of such agreements. They differ widely in scale and scope, and few of them will have any impact on the way the EU operates in matters of anti-trust policy.

However, some of them are of interest for anti-trust policy and for the application of the Digital Markets Act. The DMA is a hybrid regulation that combines ex ante regulation with tools of ex post competition policy. In some of the operations of the DMA, it will clearly be based on instruments such as market investigations and the same legal basis that applies for competition policy. Furthermore, the DMA will regulate competition aspects of platforms that are currently subject to anti-trust action in the EU, and it is highly likely that gatekeeping platforms in the future will be subject to decisions on the same subject and practice that are partly taken based on the competition regulation, the DMA and national competition law. For companies designated as gatekeeper, competition law will be based on a mix of different regulations.

There is a clear distinction between the DMA and the competition regulation as far as procedural rules are concerned. The motivation for taking action against a firm after a market investigation can be different depending on whether the EU acts on the basis of the DMA or the competition regulation. Under the DMA, actions will not require the same quality of evidence and motivation. The gatekeepers that are subject to the actions have no effective right of defence.

This may cause friction with other countries. While the bilateral agreements on competition policy between the EU and the US do not regulate the decisions that a competition authority may take, there are procedural provisions and, in the case of mergers and acquisitions, a protocol for best practice. Other agreements go further. For instance, the Trade and Cooperation Agreement between the EU and the UK has an extensive chapter on competition policy and its enforcement. It includes in Article 360 the following rule:

> *"Each Party shall apply its competition law in a transparent and non-discriminatory manner, respecting the principles of procedural fairness, including the rights of defence of the economic actors concerned, irrespective of their nationality or ownership status."*

While the specific application concerns competition law, the hybrid nature of EU decisions in matters of competition relating to gatekeepers can make this international restriction problematic for the EU. It includes references to transparency and non-discrimination, and the rights of defence of the concerned economic operator. Decisions based on the DMA could fail on at least two of these standards: transparency and rights of defence.

Services market access

A final area where there may be a risk of conflict between the digital regulations covered in this study and international trade agreements is services market access commitments that the EU has made both in its bilateral FTA negotiations and on the multilateral level at the WTO. In fact, it is likely the area that may cause the greatest numbers of concern.

A first and important level of analysis is the services bindings made by the EU under the WTO GATS agreement – basically the extent to which the EU has committed itself to market access obligations in services trade that will be affected by the digital regulations. With WTO commitments being the floor of the bilateral trade agreements that the EU has signed, concerns related to WTO violation will immediately lead to concerns over violations of provisions in the bilateral agreements. Relevant commitments that the EU has made concern informational services. These include, among others, communication services, database services, data processing services, computer and related services, and a variety of other services that are likely to be affected by all four digital regulations.

The schedule of commitments follows a positive list approach – meaning, in this case, that the EU and its Member States have specified what services that will be traded openly. The GATS schedules and commitments were negotiated at a time when digital services were not developed or much in use, and hence come with relatively few limitations. There are some limitations registered for a few individual Member States in areas such as mode 4 commitments (e.g. recognition of professional standard for a computer scientist), but generally GATS commitments made by the EU are pretty wide.[51] In effect, the EU has not detailed any limitations that are of relevance for this analysis. Hence, if one of the four regulations will deny a country market access rights, it goes against the obligations of the GATS.

However, the obligations are not the only relevant point of analysis. It is clear that, under the GATS, every WTO member has the right to regulate. In the chapeau of the GATS agreement "the right of Members to regulate, and to introduce new regulations, on the supply of services within their territories in order to meet national policy objectives" is directly recognised.[52] While this is an important qualification, it does not provide members with a right to discriminate against others or violate the principle of likeness – or "like service". The question, therefore, is how these two aspects – the right to regulate and the principle of likeness when a binding has been made – should be viewed against each other.

[51] WTO (2019) European Union. Schedule of Specific Commitments.

[52] WTO (2023) General Agreement on Trade in Services.

Anyone bringing a case against the EU will first has to establish that there is discrimination. Given how the DMA and the Data Act are designed, it is likely they will result in different treatment of services and services suppliers. Some services and suppliers will have access to the EU market for its full range of platform services; others will not. Under the DMA, a gatekeeping platform will likely be barred from certain actions and will be obliged to act in ways that non-gatekeeping platforms are spared. In the language of trade law, this is discrimination – even if the actual regulation does not specify certain countries whose economic operators will be discriminated. The fact that a like service will be treated differently depending on who markets the specific service is plain discrimination.

There has not been any extensive development of jurisprudence or rules to determine likeness in GATS. Obviously, GATS draws from core GATT rules on likeness, but there is a crucial difference. While GATT rules on national treatment only refers to "like products", GATS includes not just the product – the service – but also "the service suppliers". Hence, the likeness obligation includes both the product and the producer – which is natural given the intangibility of services and difficulties to separate the service from the supplier. While this rule has been interpreted in various ways, it is clear GATS provide a potentially bigger hurdle for the EU if its digital regulations discriminate both services that are like and services suppliers that are like.

Obviously, the EU could defend its regulations and claim that either there is no de jure discrimination or that discrimination is legitimate. For instance, the EU could argue that, even if the regulations could result in discrimination, there is no discriminatory intent, and that the discrimination of like services is de facto and simply an effect of legitimate regulatory activity by the EU.

However, both approaches will encounter problems, even if a final analysis would have to start from the actual or applied form of any discriminatory action. What complicates the matter is, first, that the "revealing architecture" or the "revealing structure" of the EU regulations, is focusing predominantly on foreign companies operating in the EU. The intent of individual regulations as well as their combined effect make it clear that EU legislators have predominantly been occupied by firms of another country and, possibly, that the designation criteria in the DMA are tailored to capture US firms without supporting evidence that a particular company has acted in ways that are problematic. There is a long trail of statements made by EU officials that support the interpretation that these regulations are intended to support the technological and digital sovereignty of the EU or that they are, in the words of Commissioner Thierry Breton "the cornerstone of a strong, innovative and sovereign European digital economy."[53] Such motivations reveal intent that sits uncomfortably with core GATS rules.

If justification via this route seems unlikely, especially as like services will be discriminated, the EU could argue that it has the right to openly deny market access on the basis of the exceptions in the WTO GATS agreement. Article XIV of the WTO GATS agreement outlines general exceptions and provides justifications for adopting or enforcing trade restrictive rules when members want to conditionally diverge from

[53] European Commission (2022) Data Act: Commission Proposes Measures for a Fair and Innovative Data Economy.

obligations that they are bound to. Justifications include the protection of public moral or maintenance of public order; human, animal or plant life or health; and securing the compliance of laws or regulations relevant for the prevention of deceptive and fraudulent practices, the protection of privacy, or safety.

These justifications for conditional departure from markets access obligations seem distant from the motivations provided for the new digital regulations. Moreover, these justifications come with requirements.[54] For example, the public order exception can only be invoked in the case if "a genuine and sufficiently serious threat is posed to one of the fundamental interests of society". In addition, there is a necessity test and there is a burden of proof for the invoking party that the restrictions are necessary.[55] Article XIV also includes a chapeau stating that restrictions cannot take the form of arbitrary or unjustifiable discrimination or that of a disguised restriction on trade in services.[56]

The GATS agreement also includes Article XIV bis on security exceptions. This article provides WTO members with exceptions to protect their "essential security interests" and for "any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security". But these exceptions also come with the requirement to inform the Council for Trade in Services "to the fullest extent possible of measures taken" and of their termination.[57] And so far the European Commission has not provided such a justification that measures are necessary to achieve the reasons under Articles XIV or XIV bis.

Another key element of the analysis are services market access commitments that the EU has made in its FTA negotiations, notably in its deep and comprehensive trade agreements with other advanced economies. Market access commitments in agreements such as those with Japan and South Korea include even stronger market access commitments than what the EU has committed to in the WTO. These agreements with Japan and South Korea include comprehensive schedules of services market access commitments that are also relevant for e-commerce. The importance of digital trade in the EU's bilateral negotiations is also highlighted by the signing of digital trade principles during the 10th Trade Committee between the EU and the Republic of Korea in November 2022.[58]

The extent to which discrimination of like services and service in the DMA and the Data Act pose a risk of conflict with these FTA commitments, however, largely depends on how the regulations will be applied in practice by the EU. The DMA and the Data Act have a variety of ambiguities, often suffer from vagueness in context, and there is not a lot of existing jurisprudence related to its area. Existing services market access commitments in comprehensive FTAs negotiated by the EU certainly include significant areas and scope for conflict with the EU's digital regulation. However, a conclusive assessment to what extent and in which specific areas there will be conflict still depends on the actual and specific implementation of the regulations by the European Commission.

[54] Springer (2013) Appendix: Justification of Trade Restricting Rules (Article XIV GATS).

[55] WTO (2023) General Exceptions: Article XIV of the GATS.

[56] WTO (2023) General Agreement on Trade in Services.

[57] WTO (2023) General Agreement on Trade in Services.

[58] European Commission (2022) EU and Korea sign Digital Trade Principles. Press Release.

6.3 Risk of retaliation

These new digital regulations – individually and collectively – have drawn the attention of other countries. Especially one country has signalled that it is unhappy about the design and effects of some parts of the regulations, even if they lend general support to their broad objectives. That country is, obviously, the US. While other countries have signalled concern too, the risk of retaliation basically comes down to one issue: will the US government respond in ways that may hurt European economic interests?

What is unique about these digital regulations is that, in their effect on foreign companies and trade rights, they all will impact on basically the same companies, the same assets and the same flows. Even if they are separate legislative acts, they concentrate in their effects. Arguably, this complicates the process and make it more likely that there will be a retaliatory response at some point. The combined effect of these regulations on a handful of companies and their business is likely to be substantial. Their opportunity to do business in Europe will be significantly curtailed, with the result that sales and profits will go down. Eventually this will impact on the broader US economy too.

It is unlikely that the US will respond by invoking rights under the GATS agreement. After all, the US has gone out of its way to make the WTO an ineffective body for settling disputes, and its own recent record rather suggests that it increasingly relies on unilateral measures. However, it can build its actions on at least plausible allegations of discrimination.

Take, for instance, the Data Act. Most provisions of the Data Act are by themselves not discriminatory by design: they impose the same burden on EU and non-EU companies. However, there are two outstanding exemptions. First, Article 5 (2) includes an exemption for core platform services of "gatekeepers" to be an eligible third-party data recipient under the Data Act data sharing regime. Second, Article 27 of the proposed Data Act includes several provisions that could severely hamper the free exchange of non-personal data to jurisdictions outside the EU.

It is clear that a gatekeeper exemption would primary hit foreign companies, especially US technology companies.[59] In addition, restrictions to the free international flow of non-personal data (such as local establishment requirements and foreign ownership restrictions as proposed by the EUCS) would by design discriminate against foreign businesses, primarily US providers. The three largest US technology companies together account for 72 % of the EU cloud market share.

Failure to meet US demands on market access for US-headquartered data and data services providers could result in significant retaliatory measures based on Section 301 of the Trade Act of 1972. Obviously, the same goes for other EU digital regulations that may come with serious harm on US companies. To "eliminate an act, policy, or practice" that discriminates against US-based companies, the US Trade Representative can "impose duties or other import restrictions on the goods of, and, notwithstanding

[59] See, e.g., Gary Clyde Hufbauer and Megan Hogan (2022) The European Union renews its offensive against US technology firms. PIIE.

any other provision of law, fees or restrictions on the services of, such foreign country for such time as the Trade Representative determines appropriate". Section 301 can be a powerful tool when the US administration is willing to fully use it.[60] The US recently considered imposing retaliatory tariffs against four EU countries that implemented discriminatory taxes on digital services provided by US technology companies. Retaliatory tariffs would have covered approximately USD 3.0 billion worth of traded goods annually (see Table 6.1).[61]

Depending on political preferences, the US administration could respond in kind and, contrary to measures against EU digital services measures, expend the scope to new technologies and business models, such as IoT in the energy and healthcare sectors and autonomous driving in the transport sector. The value of affected EU imports to the US will critically depend on the actual restrictiveness and impacts on market access to the EU.

Table 6.1. US retaliatory tariffs to Digital Services Taxes (DSTs) imposed by EU countries.

	US retaliatory Tariffs to Digital Services Taxes imposed by EU (28) countries				Share in EU-US services trade	
Country	**Affected items**	**Value of Affected USUS Imports (2019)**	**Tariff Rate**	**Tarif cost burden**	**Share in EU28 services exports to US**	**Share in EU28 services imports from US**
Austria	glassware, binoculars, refrigerators etc..	65,207,231	25 %	16,301,808	0.70 %	0.80 %
France	cosmetics, handbags etc.	1,296,969,068	25 %	324,242,267	9.70 %	8.60 %
Italy	textiles and footwear etc.	385,757,538	25 %	96,439,385	3.30 %	3.80 %
Spain	sea food, textiles, footwear etc.	323,435,820	25 %	80,858,955	3.10 %	2.10 %
UK	textiles, footwear, furniture etc.	886,553,092	25 %	221,638,273	30.60 %	17.90 %
Total		**2,957,922,749**		**739,480,687**	**47.40 %**	**33.20 %**

Source: USTR announcements on Section 301 – Digital Services Taxes, available at https://ustr.gov/issue-areas/enforcement/section-301-investigations/section-301-digital-services-taxes. Trade data from Eurostat.

[60] The motivation behind creating and strengthening mechanisms for potential retaliation had been primarily to expand US export opportunities and to induce other nations to reduce trade barriers – not to punish or inflict economic harm on trading partners. There have been 130 cases under Section 301 since the law's enactment in 1974, of which 35 have been initiated since the WTO's establishment in 1995. Historically, section 301 cases have targeted primarily the EU, which accounts for about 30 % of all cases – concerning mostly agricultural trade.

[61] Austria, France, Italy and Spain, and the UK, which has left the EU. On October 21, 2021, the US announced it will terminate tariffs it had threatened against Austria, France, Italy, Spain, and the United Kingdom in exchange for removing digital services taxes imposed on large US technology firms. See USTR (2021) USTR Announces, and Immediately Suspends, Tariffs in Section 301 Digital Services Taxes Investigations, 2 June.

It could also create a motivation for action that is not explicitly about discrimination. The AI Act, for instance, is not by itself discriminatory in the sense that it imposes the same burden on EU and non-EU companies. However, by regulating the AI supply chain and imposing these obligations on non-EU companies in case of non-compliance, the AI Act will lead to higher costs for non-EU companies wanting to place their AI systems on the EU market. Given EU's economic integration with the US and their leading role in the development and deployment of AI technology globally, these new costs will fall squarely on US companies.

Notably, in the case of AI technology, the denied market access in the EU market will affect other US companies than the big technology firms. The US is the largest investor in AI technologies, the country with the largest AI unicorns, both in terms of numbers (292 AI unicorns) and value (€3.8 trillion), and with the largest number of AI published scientific paper.[62] AI was fostered in the technology sector, but it has quickly proliferated to many other sectors such as manufacturing, healthcare, and insurance, with leading US technology companies offering customized AI tools and capabilities to clients through cloud-computing.[63] European companies are using AI to create their quarterly reports or generate images for marketing purposes. GPT-3, the leading general-purpose AI system, operated by US company OpenAI, has been integrated in hundreds of downstream applications, some of them produced by European companies. For example, Netherlands-based MessageBird offers an omnichannel communications platform which is powered by GPT-3, and Finland-based Flowrite turns sequences of words into ready-to-send emails, messages, and posts.[64]

The emergence of an EU-US AI ecosystem is the reason why, even though imposing costs on US companies is likely to lead to a response, the main cost to the EU economy will be self-inflicted. As mentioned previously, by regulating the AI supply chain, the AI Act risks driving a wedge between the EU economy and its main source of AI technology. The danger is that the EU will stop having access to the most advanced AI systems produced outside the EU, hurting EU's productivity growth and its economic prosperity. This is particularly relevant for sectors like pharmaceuticals or medical technology, where EU companies currently enjoy a leading position, but where AI systems will become a much more critical part of the innovation process.

The AI Act, together with the other digital regulations, throws a spanner in the works of the EU digital economy. For instance, it is already more difficult to get personal data from the EU into other markets as a result of the GDPR and the upcoming Data Act creates additional requirements and restrictions for non-machinery generated non-personal data. These limitations, coupled with the new obligations from the AI Act, are likely to impact on the development of AI within Europe, for instance by distancing EU companies from the latest AI systems and making collaborations with non-EU companies at the frontier of AI technology more complicated.

[62] Nathan Benaich and Ian Hogarth (2022) State of AI Report.

[63] The Economist (2022) Artificial Intelligence is permeating business at last. Retrieved from: https://www.economist.com/business/2022/12/06/artificial-intelligence-is-permeating-business-at-last

[64] Future of Life Institute (2022) Emerging Non-European Monopolies in the Global AI Market.

EU's unilateral approach in the AI Act could also affect its conversations with foreign countries on digital regulations. For instance, the EU is part of two Trade and Technology Councils with India and the US. By implementing the AI Act, which already contains specific rules and definitions, the EU could essentially close certain doors for collaboration in these councils. And even if the EU could convince some countries to follow its approach to regulating AI, there is no adequacy mechanism – like in the EU GDPR – or a Mutual Recognition Agreement that lowers regulatory costs by making compliance with another country's regulation akin to complying with the EU AI Act. Efforts to regulate AI should be accompanied by policies that search for ways to achieve cross-border integration. Standards are certainly part of that work, and their role should be underlined as the EU moves to finalise its AI regulation. Making it easier to "dock" with the EU system would likely reduce the risk that other countries will retaliate.

7. Conclusion

For a number of years, the EU has been increasingly concerned about its digital economic performance and the risk that it is not at the frontier of digital innovation and data-driven technological change. The leading companies in the digital space are often non-European and usually American, and the entrepreneurial dynamism that has driven firm growth and technological change in the US have not been mirrored in Europe. While the EU is a mix of countries with different digital profiles – and with some clearly closer to the technological frontier than others – there has been a growing assumption in EU policy recently that EU needs to build technological or digital sovereignty, and that its dependence on US technology is a threat to strategic economic autonomy.

A parallel development in EU policy is that digital change is coming thick and fast, and that a vast array of new regulations is necessary to avoid undesirable consequences of digitalisation. The concentration of online business to some platforms has naturally triggered concern – just as they have elsewhere – that the digital economy is a "winner-takes-all" market that will cement a market structure with only a few companies at the top who are able to compete. Business practices that have hindered interoperability of devices and apps, and that have pushed unfair contracts and business terms upon third party users, have provided reason for regulation of platforms and data. There has also been a new case for improved consumer protection and privacy – cutting through various forms of new digital regulations. The risk that we are creating new and powerful models of software and data programmes that no one will be able to control have added new justification for advancing ethical norms and regulations. The AI Act is a case in point.

It is clear that the four regulations covered in this analysis mix both types of motivation listed above – the case for technological sovereignty, on the one hand, and concern for fairness and reasonable protection, on the other hand. This may or may not be a good mix – and the purpose of this study has not been to give an up-or-down judgement of the regulations. But, harking back to the principles of good regulation that we started with in the introduction, it is easy to observe that the purpose, design, and structure of the four regulations are a bit messy and that the process for their introduction has been untidy.

The **Digital Markets Act**, restricting the commercial and data operations of "gatekeeping" platforms, is built on solid but abstract economic motivations that never really find a clean reflection in the design and structure of the regulation. It is an incredibly complex and non-transparent regulation, and it is impossible to know exactly how it will operate in the future and how it will be used in sharp cases. Speed has obviously been given stronger priority than substance in the regulatory process,

and it is remarkable that the Impact Assessments of the proposal was so thin on economic analysis. It may be a regulation that will have significant and positive effects on the EU economy and, at the least, give new opportunities for competition and contestability in Europe's digital markets. But it is equally plausible that it may not. What safely can be said is that, when designing the regulation, EU lawmakers were flying as much in the dark as everyone else.

The **Digital Services Act**, which regulates important digital services, is cleaner and neater than the DMA. It also builds on an already existing directive and various codes of conduct that have been developed between the Commission and big platforms over several years. It is likely that the administrative costs of the regulation will be far higher than estimated by the Commission; it is equally likely that there will be some unwanted downstream dynamic effects that will slow down the digitalisation of retail, especially for micro and small firms, and make it costlier for businesses to contract with customers on platforms. However, these effects are predictable and, compared with the potential effects of the other regulations, most likely smaller. They can also be balanced with typical Single Market benefits – a reduction in fragmentation costs – provided that the Commission and the courts are prepared to keep Member States on a tight leash.

The **AI Act**, which will regulate the AI process and the involved operators, has not yet been agreed and there is, at the time of writing, different iterations discussed. On the basis of the principles of good regulation outlined in the Introduction, and the EU's own policy for Better Regulation, it is warranted to raise some concerns about the act. They were already reflected in the review of the regulatory proposal by the Regulatory Scrutiny Board, and, in fact, the problems have exacerbated since then. It is motivated with regulation that prompts an ethical regime upon the development of AI and the evolution of the market if it can be done in a way that avoids creating huge costs and other burdens for companies. However, the act has some basic design problems with the concepts of data and AI – ultimately what it is that should be regulated. It is far from clear what this regime will cover in practice, and the current iterations into General Purpose AI Systems has not made that easier. The cost implications of the regulation are equally unclear – as is downstream effects on EU businesses and their innovation, and how the AI value chain will be impacted. What can be said, though, is that the Commission's attempt to estimate these effects is deeply unsatisfactory. In fact, some of the assumptions and estimations in the Impact Assessment – e.g. the estimation that firms will need only three minutes to read and understand the obligations in the AI Act – are so unrealistic that they are almost farcical.

Finally, the **Data Act**, which aims at providing more data access and sharing, is also unfinished, and it remains to be seen how key provisions will be designed. While there are some commonly acknowledged justifications for some elements of the Data Act – and the broader ambition to facilitate data sharing – it is the regulation that has the weakest stated objective. In fact, it is often unclear why there is a motivation to act and how the specific provisions reflect these motivations. Often, it is not clear that there is a problem that needs fixing, or a problem that can be fixed if the EU wants to build its economy on market economy principles and institutions. Equally, key concepts in the Data Act – like data, data holder, and compensation – are ambiguous

and have caused a substantial amount of confusion in the expert community. Just as with the other three regulations, the regulatory process has not invited authority and the Impact Assessments are inadequate.

There are some common threads that bind this analysis together. One, referred to in all the regulations above, is the lack of adequate economic analysis of the proposals – a problem that is exacerbated by the fact that many regulations are significantly changed after the Commission has made its proposal. Administrative and implementation costs are routinely underestimated. It has been well established by evaluations of the GDPR that these costs were far higher than what the Commission initially had estimated. In fact, these evaluations suggest a completely different order of cost magnitude, and that it is just not a one-off cost but something that repeatedly effects corporate financial planning. A proper regulatory process would at least start with a realistic view of these types of costs.

A second common thread is the absence of serious attention to consequences for trade and trade policy – or for Europe's international obligations – of these four regulations. Given the stated ambition to build technological sovereignty, one would have thought that the Commission would have made more efforts to show that it does not want to discriminate and violate the rules of the WTO, and that it has an intention to "internationalise" compliance with the regulation – meaning, making it easier for foreign companies operating under different regimes to "dock" with EU regulations without causing significant regulatory costs. These aspects are routinely missing in the Impact Assessments, despite the Commission knowing that it is trespassing in difficult territories as far as trade law is concerned.

Moreover, Europe has ambitions to cooperate with other countries in matters of digital or digitally enabled trade, and identified in its trade strategy that there are possibilities for the EU to improve on the trading conditions for many EU based firms that exchange services globally. Obviously, as one of the biggest global traders, the EU has a big interest to ensure that European companies that engage in various forms of digital trade are not confronted with severe market-access restrictions and rules that prohibit exchange. However, the risk is that the EU's own digital regulations will have an impact on the ability to negotiate with other countries. The exact design of digital regulations is therefore important for EU trade policy: how regulations are structured matters crucially for how compatible they are with trade policy. Absent a proper analysis of trade policy in the Impact Assessment, the EU has effectively been downgrading its trade-policy ambitions.

A third common thread is that many of these regulations steps into complex legal areas with consequences for intellectual property rights, trade secrets, and other commercial forms of protecting assets. The intangible economy is different from the tangible economy. In the new intangible economy, the forms of protecting assets build on several forms of legal institutions. To protect investments in technologies and services for creating, organising, and storing data – and to use it for commercial purposes – companies need to mix protective rights and contracts. Since most companies involved in the data sector "share" a lot of data, there needs to be clear protections of assets and investments. In the past, the EU has observed these

complexities and refrained from regulations that may bring unintended consequences for intangibles protection. Now it rather seems as if the EU is less restrained and is prepared to upend the system. If that is an intention, or an acceptable consequence, it should at the least analyse what the consequences may be for the European economy.

A fourth common thread is that both proposals and final versions of regulations are complex and add a lot more complexity to a complex economy. Often, key concepts in the four regulations are open to different interpretations and it is sometimes clear that vagueness is intentional. In an optimistic scenario, there will be an attendant process to establish standards that will alleviate the complexity of the regulations and bring clarity to key concepts. However, that may not happen – at least in all necessary areas – and one could argue that the legislator should make greater efforts to propose and adopt regulations that are readily understandable and avoid creating more complexity and uncertainty.

A fifth common thread is that the EU would have benefitted from more than just one initial Impact Assessment of one single digital regulation. Notably, all the four digital regulations have changed profoundly in the process from conception to their final stages. The resulting regulations vary substantially from the version of the regulations that were subject to the assessments, but no additional analyses of their effects were made along the way. This is not a good order. There is a pretence of knowledge about the regulatory consequences, but the real effects – emerging when the regulations get into force – are different because the regulations had changed. Yet such problems could be reduced by having a regulatory process that allow for more assessments along the way. Building on the OECD's work on good regulations for new technology, it is important to have feedback loops and adjust policy on the basis of new knowledge.

In addition, the Impact Assessments covered only the potential effects of one regulation while there are many regulations developed at the same time that will impact on exactly the same companies, business models, trade flows, and data assets. For instance, the Data Act links up with the DMA but there has been no attempt to understand how the DMA will influence the data that the Data Act targets. It is obvious that the actual effect of the Data Act will partly be shaped by the design of the AI Act, and how the data value chain will have to be re-structured to fit with the AI Act. While focused and highly specific analyses may generally be advisable, it is clear that the absence of broader analytical approach (encompassing more than one regulation) has made the EU less capable of understanding the consequences of its regulations.

The absence of adequate analysis begs the question: is it the intention of the EU to make global digital and technological integration harder, and ultimately create a digital economy where the EU increasingly develops and produces for itself? Clearly, the presentation of and public motivation for these regulations have been on the muscular side, and representatives of the Commission have certainly fuelled suspicions that the end goal is more about industrial policy than boosting competition, fairness, contestability, and ethical behaviour. The fact that several of these regulations are unpredictable, and that we may face some really unwanted economic consequences of them in the decades to come, adds other concerns of a careless attitude to regulation.

The net result may be that European companies and users will be deprived of access to frontier technology, and that they may not have the same capability to compete in the future. Often, the effect of technology regulation is that the cost of using technologies will go up and thus slow down the pace of technological change. If the technology is predominantly developed elsewhere, regulations that create a gap between the EU market and world market are clearly at risk of creating supple problems. In the long sweep of economic history, the pace of growth and the relative position of one economy vis-à-vis other economies are defined by the proximity to the technological frontier and the quality of economic institutions. The EU is now making the bet that tougher digital regulations in Europe than in other advanced markets will not slow its relative pace of technological change. It may be proven right. It may also be proven wrong.

www.svensktnaringsliv.se
Storgatan 19, 114 82 Stockholm
Phone 08-553 430 00

Print: Arkitektkopia AB, Bromma, 2023