An EPICENTER report

DIGITAL REVIVAL?

How regulation prevents the rise of European tech leaders

Edited by Carlo Stagnaro and Christian Năsulea

February 2025

EPICENTER
European Policy Information Center

Contents

Summary **6**

Introduction **10**

The absence of European tech leaders **13**

General Data Protection Regulation **19**

Digital Services Act **27**

Digital Markets Act: The theoretical background **35**

Digital Markets Act: How to improve it **44**

The EU's AI regulations:
Fostering innovation and upholding freedom of expression **47**

References **56**

About the authors and editors

Carlo Stagnaro is the Director of Research and Studies at Istituto Bruno Leoni. He was previously the Chief of the Minister's Technical Staff at Italy's Ministry of Economic Development. He holds an MSc in Environmental Engineering from the University of Genoa and a PhD in Economics, Markets, and Institutions from IMT Alti Studi, Lucca. He is also a member of the Academic Advisory Council of the Institute of Economic Affairs and a Fellow of the Italian Observatory on Energy Poverty at the University of Padua's Levi-Cases Centre. He is a member of the editorial boards of the journals Energia and Aspenia. His main research interests include energy economics, competition policy, regulation, and digital markets.

Contact: constantinos.saravakos@kefim.org

Cécile Philippe (PhD) is an economist, writer, and think-tank president. She is interested in systemic issues and projects with great economic and social impact and is keen to foster freedom, prosperity, and well-being. She has led the Institut économique Molinari since its founding in 2003, working to implement consensus-based and pragmatic institutional solutions to national and worldwide challenges.

Contact: cecile@institutmolinari.org

Piotr Oliński is a legal analyst at the Civic Development Forum (FOR) and a PhD student at the University of Gdańsk. He specialises in competition law, economic constitutionalism, and administrative law.

Contact: piotr.olinski@for.org.pl

Christian Năsulea (PhD) teaches economics at the Faculty of History at the University of Bucharest and is an associate lecturer at the Faculty of Business Administration in Foreign Languages at the Bucharest University of Economic Studies. He is also the executive director of the Institute for Economic Studies – Europe and a fellow of the Institut de Recherches Économiques et Fiscales. He holds a doctor's degree in management with a thesis on complex adaptive systems. His research interests revolve around economics and technology. In addition to his academic work, he is also a tech entrepreneur, currently holding CEO or CTO positions in several tech businesses.

Contact: c.nasulea@ies-europe.org

Giuseppe Colangelo is a Jean Monnet Professor of European Innovation Policy and an Associate Professor of Law and Economics at University of Basilicata (Italy). He also serves as Adjunct Professor of Markets, Regulation and Law at LUISS (Italy). He is fellow of the Stanford Law School and University of Vienna Transatlantic Technology Law Forum (TTLF), the scientific coordinator of the Research Network for Digital Ecosystem, Economic Policy and Innovation (Deep-In), and an academic affiliate with the International Center for Law & Economics (ICLE). His primary research interests are related to competition law and policy, market regulation, innovation policy, intellectual property, and economic analysis of law.

giuseppe.colangelo@unibas.it

Patryk Wachowiec is a vice-president of the Civil Development Forum Foundation (FOR) and is responsible for the Rule of Law branch. His main areas of expertise include the organisation of the judicial system, the independence of the judiciary, and freedom of information. He has previously worked for the Bureau of Research in the Polish parliament, the Bingham Centre for the Rule of Law (London), and the National Board for Legal Advisers.

Contact: patryk.wachowiec@for.org.pl

William Hongsong Wang (PhD) is the head of research at the Fundación para el Avance de la Libertad (Fundalib) and an assistant professor of economics and director of Official Master Degree of International Trade and Economic Relations at Universidad Europea de Madrid, Spain. His research interests include environmental economics (free-market approach), the history of economic thought, economic history, entrepreneurship, and public policy. He has served as a consulting author for many reports on Spanish and EU public policy for think tanks and frequently attends related events and conferences.

Contact: h.wang@fundalib.org

Summary

The long-run causes of the absence of EU tech leaders

- The absence of European tech leaders has become a feature of Europe's industrial landscape. It is the symptom of an entire continent unable to drive innovation in sectors that are of immense value at present, i.e., information and communication technologies.
- One key factor is the lack of long-term savings in the EU and the absence of a major European stock exchange. The EU has a market capitalisation deficit of €10.4 trillion when compared with the OECD (Marques and Portuese 2023).
- These financing issues should prioritised to address the EU's inability to fund innovation.
- On top of financing, the EU has introduced large bodies of regulations aimed at making Europe a sort of regulatory superpower. These regulations often aim to protecting users and promoting competition, but introduce burdensome obligations that may hinder, rather than promote, economic dynamism. In some cases, they even discourage the adoption of innovations or the experimentation or development of new technologies. In the following, the main such regulations are considered – the GDPR on personal data, the DSA and DMA about large online platforms, and the Artificial Intelligence Act – and potential improvements or revisions are suggested.

General Data Protection Regulation (GDPR)

- In order to make the GDPR less distortionary, a streamlined compliance framework specifically for small and medium-sized enterprises (SMEs) and start-ups in data-intensive sectors should be developed. This

framework could include targeted exemptions from certain GDPR requirements, such as extensive consent mechanisms in contexts involving low-risk data processing, particularly for small companies dealing with AI, machine learning, and digital innovation. By reducing the compliance burden on emerging businesses, this initiative would level the playing field with larger corporations, fostering innovation without compromising privacy.

- Guidelines should be issued that clarify acceptable forms of data-sharing arrangements among businesses. Establishing a regulatory 'safe harbour' for innovation-friendly data-sharing practices, such as the sharing of anonymised data sets, would enable businesses to develop new services within privacy standards. This approach would be especially valuable in sectors such as healthcare and finance, where data-driven solutions offer substantial benefits for consumers.
- Reduced-cost compliance pathways for SMEs, including standardised templates and simplified record-keeping for GDPR documentation, should be implemented.
- To mitigate fragmented enforcement, the EU Commission should work to strengthen the role of the European Data Protection Board (EDPB) by granting it central oversight in cross-border case management and binding decision-making powers. This would reduce compliance uncertainty for businesses operating across multiple EU countries, ensuring consistent application of the GDPR standards throughout member states.
- Evaluate the economic impact of the GDPR on EU competitiveness and advocate for adjustments that lower regulatory barriers in the digital economy. This could involve proposing data processing exemptions in sectors critical to economic growth, such as fintech and digital trade, where controlled data flows are essential. Additionally, the EU Commission could support the establishment of a 'sandbox' environment for innovative digital services, allowing controlled experimentation with data-driven solutions within the GDPR oversight.

Digital Services Act (DSA)

- The Digital Services Act (DSA) deals with online commerce and user-generated content. The concept of 'illegal content' is central to the application of DSA. For example, Article 23 of the DSA requires providers of online platforms to suspend 'recipients of the service that

frequently provide manifestly illegal content'.An expansive interpretation of 'illegality' would lead to the notorious social media phenomenon of over-blocking.

- The concept of illegal content should be better specified. This clarification could initially come in the form of guidelines promulgated by the European Commission (hereinafter, the Commission) – such as the guidelines for 'very large' online platforms (VLOPs) and search engines (VLOSEs) on the mitigation of systemic risks for electoral processes, which were released in April 2024 – explicitly pointing out how over-blocking contradicts the DSA, which prohibits explicitly illegal content. Ultimately, consideration could be given to clarifying the riskiest provisions in this regard and perhaps expanding the definition of 'illegal content'. This should be done in line with future Court of Justice of the EU (CJEU) case law.
- Adopting a human rights–based approach to blocking content will foster legal certainty by referring to the standard derived from current jurisprudence. This approach can be taken by the Commission both in specific proceedings and in soft-law documents clarifying the provisions of the DSA. In order to prevent the suspect of a political use of the DSA, an independent digital markets unit responsible for the enforcement of the DMA (see below) and DSA should be considered, as well as other acts relating to the digital economy.
- The Commission should review the reporting obligations imposed on intermediary services for proportionality after a year or two of the DSA's enforcement.

Digital Markets Act (DMA)

- The Digital Markets Act (DMA) was introduced to deal with the behaviour of large online platforms deemed as "gatekeepers", as if the existing antitrust powers were not enough to ensure that anti-competitive conducts are not put in place. Currently, the Commission, which is both an administrative and a political body, is responsible for enforcing the DMA. This situation may raise doubts about the independence of the application of the DMA – a remark that applies to both the DSA and classic competition law at the EU level. In the long run, the establishment of an autonomous digital markets unit responsible for the application of the DMA and DSA seems worthy of consideration.

- The Commission should monitor the enforcement of the DMA by private players, as this could complement the administrative measures taken by the Commission and national-level authorities. Should this scope prove to be extremely modest, provisions explicitly addressing private enforcement in the DMA could be considered.
- The obligations that the DMA imposes on mergers are extremely weak, for instance, gatekeepers need only notify the Commission in this regard. Juxtaposed with tendencies to loosen the merger control regime under traditional competition law – as reflected, for example, in the Draghi report's 'innovation defence' proposal, this risks ineffective control of mergers and acquisitions in the digital economy. However, this challenge does not necessarily have to be answered by the DMA. Consideration could be given, for example, to merger control reform.
- Should the DMA prove marginally effective, there remains plenty of room for structural remedy reforms. One possible change would be to adopt a solution familiar to, say, the regulation of the energy sector or recommend some form of unbundling of related platform services.

Artificial Intelligence Act (AI Act)

- The Artificial Intelligence Act deals with the use of AI in the EU. While in principle risk-based, its enforcement may result in discouraging innovation and the adoption of sophisticated technologies in the EU. Therefore, some changes to the AI Act should be considered. These include the following.
- The AI Act often rests on vague of too broad definitions. It could benefit from clearer definitions of key terms to reduce ambiguity and ensure consistent interpretation across member states.
- Innovation in the sector of AI comes rapidly: regulations that have been designed based upon the current state of technology may fail to recognize both the risks and the opportunities stemming from innovative applications or designs. Introducing mechanisms to regularly update the regulations can help accommodate future AI advancements without requiring complete legislative overhauls.
- The effects of regulations are felt disproportionately by SMEs, that constitute the backbone of Europe's economic environment and that are often at the forefront of innovation. While regulatory sandboxes are beneficial, additional financial and educational resources could further assist SMEs in compliance and innovation efforts.

Introduction

The Draghi report on competitiveness (European Commission 2024b) argues that the economic gap between the EU and countries such as the US and China can be explained by the technological gap between them. European firms, for instance, have been unable to stay at the frontier of innovation in the information and communication technologies (ICT) sectors. Moreover, the same Report also shows that this gap has increased in recent times. This chapter delves into the determinants of this phenomenon and proposes strategies to overcome this technological slowdown (Figure 1).

Figure 1. Top 15 equity markets in the world (2022)

Stock market	Equity market capitalization at the end of 2022 (€ billion)	Zone
NYSE	22,500	Etats-Unis
Nasdaq US	15,200	United States
Shanghai Stock Exchange	6,300	China
Euronext	**5,700**	**EU (France, Belgium, Ireland, Italy, Netherlands, Portugal + Norway non EU)**
Japan Exchange Group	5,000	Japan
Shenzhen Stock Exchange	4,400	China
Hong Kong Exchanges and Clearing	4,300	China
National Stock Exchange of India	3,200	India
LSE Group London Stock Exchange	2,900	United Kingdom
TMX Group	2,600	Canada
Saudi Exchange	2,500	Saudi Arabia
Deutsche Boerse AG	**1,800**	**UE (Germany)**
Nasdaq Nordic and Baltics	**1,700**	**EU (North + Iceland non EU)**
SIX Swiss Exchange	1,700	Switzerland
ASX Australian Securities Exchange	1,600	Australia

Source: Institut économique Molinari[1].

1 Marques, N. and Portuese, A. (2023) Télécoms et innovation, donner la priorité à la création de richesse plutôt qu'à la redistribution. Paris: Institut économique Molinari.

First, it explores the long-run determinants of the research and innovation gap. This gap is traced back to the under-development of Europe's financial markets and (private) pension funds. If this is true, then one thing the EU should do is remove regulatory and other types of obstacles that prevent investors from channelling their resources towards high-risk, hi-reward sectors, such as the digital sectors. In this respect, reforming Europe's (public) pension systems might provide a boost to financial markets, as it happened in other countries where these fresh capitals were mobilised and invested while delivering both higher, more secure pensions and support to the real economy.

However, the lack of investors in innovation is not the sole cause of the bad performance of European companies in the hi-tech sectors. EU policymakers acknowledged the gap and reacted by passing large bodies of legislation under the idea that 'if we cannot innovate, at least we should regulate'. Indeed, the stated aim of many EU policies was to turn Europe into a regulatory powerhouse, under the belief that by doing so, Brussels would set a global standard that other countries would inevitably follow. Things did not go this way: on the contrary, several large online platforms reacted by not introducing in the European markets the same innovative services they were experimenting with elsewhere, to the detriment of European businesses and households.

The following section deals with the key regulations that have been introduced so far, which hinder the EU's ability to not just innovate but also adopt innovations that have been engendered overseas. In this regard, the section discusses the General Data Protection Regulation (GDPR), 2016, which set high standards for consumers' privacy. While this may appear to be a long-due way to safeguard the users' rights, excessive protection may deprive the consumers of opportunities that stem from the use of data by innovators. Further, the GDPR is riddled with bureaucratic complexities and ambiguities, which are reviewed in this section.

The Digital Services Act (DSA), 2022, is addressed next. This regulation is presumed to protect consumers online by placing digital platforms under several obligations and preventing abusive behaviour. In particular, the DSA deals with 'illegal content' but fails to define the concept. By making online platforms liable for user-generated content and adopting a loose definition of illegality, the DSA puts disproportionate burdens on online intermediaries, which may eventually react by over-blocking content. This

risk is even more substantial given the perception that DSA implementation is motivated by political goals rather than by consumer protection.

The subsequent sections focus on the Digital Markets Act (DMA), 2022. First, its theoretical foundations are discussed. Thereafter, its practical implications are explored and potential amendments are suggested. The DMA relies on the assumption that ordinary competition rules are not fit to combat harmful behaviour in digital markets. Hence, a new category of online subjects has been identified – the so-called gatekeepers, which, in practice, are the largest online platforms – that are subject to special obligations or prohibitions.

Finally, the Artificial Intelligence Act (AI Act), 2024, is analysed, considering the limits to the development and application of AI and the EU's regulations in this domain. Similar to the DSA and DMA, the AI Act employs vague definitions that complicate its implementation and render it arbitrary. Moreover, since AI is a rapidly evolving sector, the AI Act might well prevent the development and application of the most advanced technologies.

The absence of European tech leaders

by Cecile Philippe (IEM)

The absence of European tech leaders has become a feature of the EU's industrial landscape. As rightly described by Fuest et al. (2024), Europe is trapped in middle technology specialisation, which illustrates the divergence between the EU and the US. While both the US and the EU were very much invested in the automotive industry in 2003, this changed over time as the tech industry became the top R&D spender in the US. In the EU, 25 years later, the German auto industry still occupies top spots, whereas in the US, the auto and pharma sectors have been replaced by industries of the new revolution – the tech industries. The EU is stuck in the traditional auto industry, which is undergoing a major technological shift, and even in this sector, it is not leading the way. The absence of tech leaders is the symptom of an entire continent unable to drive innovation in sectors that are of immense value today – information and communication technologies (ICT).

A recent report on competitiveness (European Commission 2024b) – published under the leadership of the former president of the European Central Bank (ECB), Mario Draghi – came to this very conclusion when addressing the persistent lack of growth in the EU in comparison with the US in the last 20 years. Growth is linked to production, which depends on the overall size of the workforce and hours worked. On both criteria, the EU lags behind the US according the Draghi Report.

As emphasised by historian Adam Tooze, 'when we seek to explain labour productivity, one obvious place to look is investment. Workers equipped

with more capital tend to be more productive'.[2] At the macro level, investment has not been up to the challenge. The key reason seems to lie in the lower business engagement in R&D in the EU. According to the OECD (2024), in 2022, business enterprise expenditure in R&D was 1.39 per cent of the GDP in the EU, and respectively 2.83 per cent of the GDP in the US. Despite the EU's goal to spend about 3 per cent of the GDP on R&D, it has never been able to reach this objective, which was originally set in 2002.[3]

Many reasons have been invoked for this lack of global investment into the EU, which is particularly visible in its incapacity in 'generating new tech companies and diffusing digital tech into the economy' (European Commission 2024b: 20). One key element is the lack of long-term savings and the absence of a major European stock exchange. The successes of the UK, France, and Germany in the first industrial revolution are historically linked to the existence of a significant stock of savings, which were channelled to the benefit of infrastructure – canals, railroads, etc. – and industry. Notably, many European countries, ruined by the two world wars, chose not to redevelop their pension systems, which had been damaged by inflation and wartime confiscation of capital. To date, these countries rely almost exclusively on pay-as-you-go (PAYG) pension schemes.

In the post-war years, which were marked by administered reconstruction plans – notably, the Marshall Plan – the redevelopment of retirement savings did not appear to be a priority. In Italy, France, and Germany, small and medium enterpriseds (SMEs) and intermediate-sized enterprise (ETIs) have managed to recover by financing their incremental growth through self-financing, bank loans, or investments by insurers. However, these methods are not suitable for financing breakthrough innovations, primarily because the financing capacity of banks and investment capacity of insurers is now drastically limited by prudential regulations (Bale, Solvency, etc....). Such regulations reinforce the key role of pension funds.

2 'Chartbook 317 Draghi's view of Europe (1): Investment, R&D & the US-EU comparison', Substack, 11 September 2024 (https://adamtooze.substack.com/p/chartbook-317-draghis-view-of-europe).

3 "In March 2002 the Barcelona European Council analyzed the Lisbon Strategy and its implementation and set the target to increase the average research investment level from 1.9% of GDP today to 3% of GDP by 2010, of which 2/3should be funded by the private sector" in 'Barcelona European Council, 15 and 16 March 2002, Presidency Conclusions', CORDIS, 27 March 2023 (https://cordis.europa.eu/programme/id/EMP-BARCELONA-2002C).

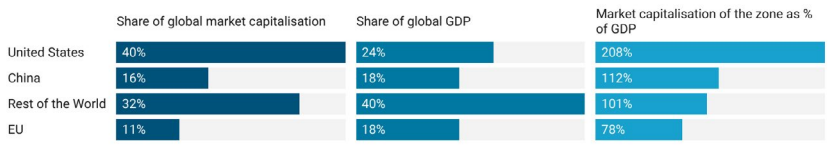
This approach has contributed to delayed growth in otherwise innovative fields, such as digital markets (e.g., e-commerce and cloud computing) and artificial intelligence (e.g., machine learning and autonomous systems), increasing European dependence and leading to a loss of sovereignty. The impressive dynamism of the American digital, tech, and telecom companies contrasts with the difficulties faced by the EU. This is partly due to the abundance of long-term savings in the US, which are further boosted by retirement savings, eventually driving innovation via the NASDAQ (Institut économique Molinari et CroissancePlus 2021).

European market capitalisations have only grown marginally over the last ten years. The EU has not only been overtaken by the US but is also losing ground to the rest of the world in equity markets, which are key to financing innovation (Figure 2). It suffers from atrophied long-term investment, which penalises the development of corporate equity. Several studies, such as Molinari and CroissancePlus (2021) and Marques and Portuese (2023) from which the data below are sourced, document this phenomenon and emphasize the importance of revitalizing the capital markets to spur innovation.

For instance, at the end of 2022, the total capitalisation of the EU stock exchanges was €9.9 trillion – roughly one-quarter the size of the American stock exchanges, which cumulatively stood at €37.7 trillion (NYSE and NASDAQ) (Marques and Portuese 2023). The largest EU stock exchange – Euronext – was one-quarter of the NYSE (traditional stocks) and one-third of the NASDAQ (technology stocks)[4]. We suspect that the problem is not one of competence – the tools and know-how are there – but of business opportunities. This problem is further exacerbated by the scarcity of long-term savings resulting from a series of ill-advised regulatory choices.

4 Stock Market Journalist, `Revealed: Largest Stock Exchanges in the World by Market Capitalization 2024`, 18 May 2024, 2024. https://stockmarketjournalist.com/revealed-largest-stock-exchanges-in-the-world-by-market-capitalization-2024/?utm_source=chatgpt.com

Figure 2. European equity markets have been outperformed by the US and China (2021)



Source: Institut économique Molinari with World Federation of Exchanges and World Bank (Marques and Portuese 2023).

The EU has a market capitalisation deficit of €10.4 trillion when compared with the OECD. At the end of 2020, the market capitalisation of European companies represented 70 per cent of the EU GDP, compared to an OECD average of 147 per cent. France – with a market capitalisation of 106 per cent of its GDP – was somewhat behind the OECD average, while other European countries were even further behind. Notable among them is Germany, with market capitalisation representing only 59 per cent of its GDP (Marques and Portuese 2023).

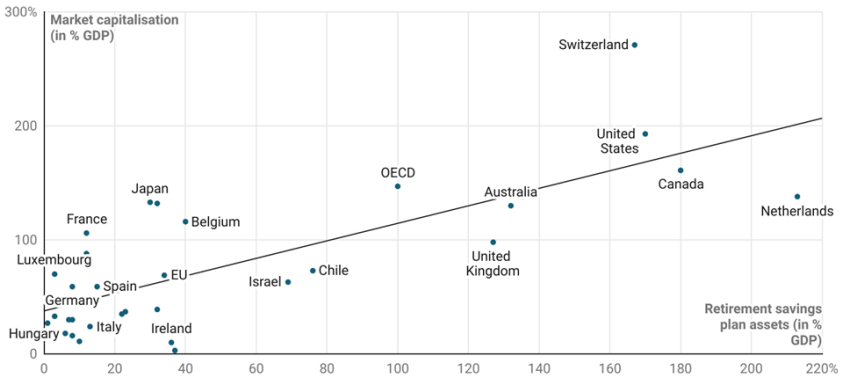
With the exception of the Scandinavian countries and the Netherlands, the EU's pension funds are underdeveloped.[5] Whereas in the rest of the world, a significant proportion of pension benefits is financed by collective or individual capitalisation based on capital invested in part in the local economic fabric, the EU benefits less from this cost-saving source of financing. Compared with the OECD average at the end of 2020, the EU had a shortfall of €8.9 trillion in long-term savings. At the end of 2021, pension funds represented 34 per cent of the GDP in the EU, compared with an OECD average of 100 per cent. The major European economies – Germany, France, Italy, and Spain – are characterised by low levels of retirement savings, representing between 8 per cent and 15 per cent of GDP. The UK, Switzerland, and Iceland, which are not part of the EU, have retirement savings representing between 127 per cent and 207 per cent of GDP. Within the EU, only Sweden, the Netherlands, and Denmark

5 The 1914–50 period, spanning World War I and World War II, was associated with inflation rates of 13 per cent and 17 per cent per annum in France and Germany, respectively, leading to a depreciation of pension capitalisation in these two countries. This was not the case in the US or the UK, where inflation rates were close to 3 per cent over this period. Figures from Thomas Piketty at http://piketty.pse.ens.fr/files/ideology/pdf/F10.10.pdf.

have retirement savings above the OECD average, with between 109 per cent and 229 per cent of their GDP invested in financing pensions (Marques and Portuese 2023).

This shortfall represents a real handicap for the equity financing of European companies. Pension funds, which hold 30 per cent of the $100 trillion invested in the stock market, are failing us in France and Europe. The connection between the development of retirement savings and stock market capitalisation is crucial. According to the OECD, about 58 per cent of the assets managed by pension funds are located in their country of origin, and the pension funds are long-term investors (Figure 3).

Figure 3. The development of retirement savings and equity market capitalisation go hand in hand (as % of GDP at the end of 2020)



Source: Institut économique Molinari with World Federation of Exchanges and OECD (Marques and Portuese 2023)

All of the above contributes to cumulative lags in technological innovation and the EU's increasing dependency on other countries. As measured by the digital dependence index (DDI, 0 being total autonomy and 1 being total dependence), Germany, France, UK, Italy, and Estonia are highly vulnerable to China for ICT goods (between 0.86 and 0.95) and when it comes to infrastructure, they depend very highly on the US (0.83 to 0.89).. According to the authors of the index "European countries are falling behind in every dimension compared to China, South Korea, and the US. […] digital interactions have become more asymmetric with China (ICT trade dependence), with the US (infrastructure and platform dependence), and the East Asian region (IP dependence)" (Mayer and Lu 2023).

To cultivate European tech leaders and prevent the EU's inability to fund innovation from turning it into a 'digital laggard' of the US and China in the long term, these financing issues must be prioritised.

General Data Protection Regulation

By Patryk Wachowiec (FOR)

The GDPR is one of the EU's most ambitious pieces of legislation in the last decade. By imposing strict requirements on personal data processing, the GDPR aims to secure individuals' rights to protection of personal data (Article 8(1) of the Charter of Fundamental Rights) and establish harmonised standards across EU member states. While these goals are admirable, the GDPR's application has introduced unintended challenges that extend beyond data protection and impact economic freedom, competitiveness, and technological progress within the EU.

The GDPR's regulatory framework has proven to be fairly restrictive, with significant implications for economic activities and innovation. Considerable operational costs – as a result of the regulation's demanding requirements – negatively impact small and medium-sized enterprises (SMEs), which often do not have enough resources to meet these obligations effectively. Additionally, enforcement mechanisms, including the 'one-stop-shop' system[6], have resulted in divergent interpretations across member states[7], causing inconsistent application and legal uncertainty for businesses.

6 The "one-stop-shop" mechanism under the GDPR allows businesses operating in multiple EU countries to work with a single lead data protection authority in the country of their main establishment. While designed to simplify compliance and enforcement, it has faced criticism due to inconsistencies in how different member states interpret and apply the GDPR, leading to legal uncertainty.

7 DIGITALEUROPE. (2024). *The GDPR six years in: From harmonisation to alignment*, 9 February 2024, https://cdn.digitaleurope.org/uploads/2024/02/The-GDPR-six-years-in-from-harmonisation-to-alignment.pdf

This section examines the GDPR's implications for the EU's economy and competitiveness across four key areas. First, this section addresses compliance costs and regulatory burdens, with a focus on the impact on SMEs. Then, it explores the challenges to enforcement due to fragmented interpretation, highlighting the implications for cross-border businesses. Next, it examines the GDPR's effects on innovation, particularly in AI, a domain where restrictive data handling requirements impact technological progress. Finally, this section discusses the practical difficulties in implementing the individual rights guaranteed by the GDPR, such as the right to be forgotten.

Compliance costs and regulatory burden

The GDPR has introduced significant operational costs for businesses, which especially affects SMEs that lack the necessary resources for full compliance. Since it came into force, the GDPR has mandated rigorous data compliance processes, including comprehensive data mapping, documentation, regular assessments, and staff training. For SMEs, many of these requirements represent expenses that can divert some of their resources from core business activities such as innovation and growth.
The nature and broad scope of the application of the GDPR have encouraged a 'tick-box' approach, wherein companies focus on meeting formal requirements over achieving genuine data protection for their clients. The GDPR prioritises procedural obligations over meaningful privacy improvements, which turns genuine compliance into an exercise in documentation. This is particularly challenging for SMEs with limited resources, as these businesses can risk non-compliance.

For larger companies, the GDPR requirements include extensive record-keeping, consent procedures, and data protection mechanisms. The latter often means hiring a data protection officer (DPO). The DPOs – required, among others, for organisations handling large amounts of personal data – must be skilled in data protection law, which leads to additional hiring or outsourcing costs. Although these expenses are manageable for large businesses, they can be expensive for SMEs.

Non-profit organisations, which usually operate on limited budgets, are particularly strained by GDPR compliance costs. Many are forced to reallocate funds from essential projects to meet regulatory requirements, sometimes adopting minimal compliance strategies that risk penalties. This unequal burden between large and small entities raises concerns about the GDPR's proportionality and its impact on fair competition across sectors.

Further, the GDPR has unintentionally created a competitive disparity between multinational corporations and SMEs since large companies can absorb compliance costs more easily, while SMEs face disproportionate economic impacts. Such a regulatory environment favours larger players, distorting the competitive landscape.

Fragmentation and enforcement challenges

One of the GDPR's central goals was to create a harmonised framework for data protection across the EU, yet significant inconsistencies in enforcement and interpretation have emerged among member states[8]. Despite the GDPR's comprehensive design, these discrepancies undermine its purpose and contribute to regulatory uncertainty for businesses operating across multiple jurisdictions. The one-stop-shop mechanism, which is intended to streamline compliance, has faced criticism[9] for not delivering the anticipated benefits of unified oversight.

Under the one-stop-shop principle, companies operating in multiple EU countries should, theoretically, have a single lead supervisory authority, usually based in the country of their main establishment. In practice, however, differences in national interpretations and enforcement priorities have led to fragmented application of the GDPR. This fragmentation is particularly evident in high-profile cases involving major technology companies. For instance, Ireland's Data Protection Commission, which oversees several large tech firms, has invited criticism (Irish Council for Civil Liberties 2021) for slow response times and perceived leniency. Such disparities have prompted other national regulators, including those in France and Germany, to question Ireland's approach, complicating the enforcement landscape further.[10]

8 DIGITALEUROPE. (2024). *The GDPR six years in: From harmonisation to alignment*, 9 February 2024, https://cdn.digitaleurope.org/uploads/2024/02/The-GDPR-six-years-in-from-harmonisation-to-alignment.pdf

9 John O'Connor, Rachel Hayes, Conor Forde, ` Stricter Rules for the GDPR's One-Stop-Shop?`, 11 April 2024, https://www.williamfry.com/knowledge/stricter-rules-for-the-gdprs-one-stop-shop/?utm_source=chatgpt.com

10 Simmons+Simmons, 'Ireland's balance between Big Tech and data privacy', 4 October 2021, https://www.simmons-simmons.com/en/publications/ckucpnrme21dy0a42mwuhhhae/ireland-s-balance-between-big-tech-and-data-privacy

This uneven enforcement not only challenges regulatory coherence but also imposes additional burdens on businesses operating across borders. Companies are often subject to varying interpretations of the GDPR, leading to inconsistent requirements. For example, data processing practices that are upheld in one member state may face scrutiny or penalties in another, creating legal uncertainty. For example, Germany did not establish one central data protection authority but authorities in each of the sixteen Länder (transl. 'countries'), which may lead to divergences in the interpretation of the GDPR[11]. Poland's supreme administrative court, unlike other member states' courts, concluded that vehicle registration plates do not contain personal data within the meaning of the GDPR[12]. French[13] and German[14] data protection authorities have expressed different approaches to the lawful use of open AI models and personal data protection. The GDPR aims to create a harmonized framework for data protection across the EU, facilitating a single digital market where businesses can operate seamlessly. However, inconsistent enforcement and varying interpretations of the regulation among member states undermine this objective. Businesses face legal uncertainty and increased compliance costs as they navigate differing national rules, making cross-border operations more complex. This fragmentation deters investment, limits innovation, and weakens the EU's competitiveness in the global digital economy, counteracting the GDPR's goal of fostering an integrated digital market.

Another challenge lies in the limited resources and expertise available to some national supervisory authorities, particularly in smaller member states, such as Slovenia[15]. These countries often lack the financial and technical capacity to handle complex data protection cases involving multinational corporations, leading to either reliance on larger states or delays in enforcement. Without adequate resources, many supervisory

11 DLA Piper, ` National Data Protection Authority. Germany`, 19 January 2024, https://www.dlapiperdataprotection.com/index.html?c=DE&t=authority&utm_

12 Squire Patton Boggs, ` Data Protection Update for Poland`, 21 July 2019, https://www.privacyworld.blog/2019/07/data-protection-update-for-poland/

13 CNIL, ` AI: ensuring GDPR compliance`, 21 September 2022, https://www.cnil.fr/en/ai-ensuring-gdpr-compliance

14 Sylvia Lorenz, Detlev Gabel, ` AI implementation & data protection regulation: German authorities publish guidelines for implementing AI in compliance with the GDPR`, Whitecase, 28 May 2024, https://www.whitecase.com/insight-our-thinking/ai-implementation-data-protection-regulation-german-authorities-publish

15 Marko Frantar, Miriam Gajšek, ` Better late than never: Slovenia last EU Member State to adopt GDPR implementing act`, schonherr, 19 January 2023, https://www.schoenherr.eu/content/better-late-than-never-slovenia-last-eu-member-state-to-adopt-gdpr-implementing-act

authorities may struggle to interpret and apply the GDPR consistently, exacerbating the existing fragmentation.

The regulatory fragmentation and inconsistent enforcement of GDPR indicate a need for greater harmonisation and resource-sharing among member states. Strengthening the role of the European Data Protection Board (EDPB) could help coordinate cross-border cases and provide more consistent guidance. However, this would require balancing national sovereignty concerns, as member states may resist ceding more power to a central EU authority.

Innovation and technological development

While the GDPR aims to safeguard personal data, its restrictive approach has affected innovation[16], especially in emerging technologies such as AI and big data analytics. These fields depend on massive amounts of data to develop, train, and optimise algorithms. Therefore, access to diverse datasets is crucial for their progress. However, the GDPR's data minimisation and purpose limitation principles restrict data collection and reuse, limiting the potential of technologies that could drive substantial social and economic benefits[17].

The data minimisation principle poses a fundamental challenge for AI developers, who need large datasets to improve accuracy and functionality. The GDPR requires that only data strictly necessary for a specific purpose be collected. However, AI systems must be flexible so they can be adapted to unanticipated applications. Consequently, the GDPR's restrictions hinder the development of AI and machine learning models that rely on continuous, expansive datasets, thereby reducing the EU's competitiveness. In contrast, countries such as the US and China, with less stringent data regulations, are advancing rapidly in AI and big data and gaining a global advantage[18]. The GDPR further presents challenges for research and development since

16 Ryan Preston, Stifling Innovation: How Global Data Protection Regulation Trends Inhibit the Growth of Healthcare Research and Start-Ups, 37 Emory Int'l L. Rev. 135 (2022). Available at: https://scholarlycommons.law.emory.edu/eilr/vol37/iss1/4

17 Cornelius Witt, Jan De Bruyne, The interplay between machine learning and data minimization under the GDPR: the case of Google's topics API, *International Data Privacy Law*, Volume 13, Issue 4, November 2023, Pages 284–298, https://doi.org/10.1093/idpl/ipad020

18 Daniel Castro, Michael McLaughin, ` Who Is Winning the AI Race: China, the EU, or the United States? — 2021 Update`, Center for Data Innovation, January 2021, https://www2.datainnovation.org/2021-china-eu-us-ai.pdf?utm_

its stringent consent requirements restrict access to large datasets necessary for effective big data analysis. Big data analytics drives innovation across sectors such as healthcare and finance by leveraging diverse datasets to identify trends. However, the GDPR's consent requirements make it difficult for researchers to collect data for longitudinal or secondary analysis. This constraint particularly impacts European research institutions and businesses, limiting their contributions to breakthroughs in data-intensive fields.

The requirement for explicit consent further complicates data use, as repurposing existing data often conflicts with original consent parameters. In dynamic fields such as AI, new consent for each data repurposing can be seen as excessively burdensome and can reduce data quality if individuals withdraw consent – if it is technologically possible – leading to incomplete datasets. European firms are disadvantaged compared with international competitors operating under flexible data policies that better accommodate modern technological needs For example, EU firms face costly procedures and redtape to acquire the users' consensus to manage personal data and are not allowed to make automated decisions based on the users' personal data. This means European companies – differently from their foreign competitors – are required to employ humans reviewing automated decisions and must explain the users how such automated decisions are made.

Additionally, the GDPR's limitations on cross-border data transfers impede cloud computing and digital services, which rely on global data flows. The regulation requires that data remain within EU-approved jurisdictions or meet comparable standards, complicating operations for multinational firms and hindering collaborative research. Data localisation requirements, while intended to protect privacy, discourage international collaboration, slowing the adoption of innovative technologies developed outside Europe.

Moreover, the compliance costs under the GDPR disproportionately affect start-ups and smaller tech firms, which are often the drivers of innovation. Unlike large corporations that can absorb compliance expenses, smaller companies may find the GDPR's demands economically unfeasible. This compliance burden stifles entrepreneurship, discouraging innovative start-ups from establishing within the EU, where regulatory costs act as a barrier to entry. Consequently, the GDPR may unintentionally favour established corporations over new entrants, hindering technological diversity and economic growth within the EU.

Finally, the GDPR's restrictive data policies can discourage foreign investment in the European tech sector. As global investors seek favourable regulatory environments, the EU's stringent framework may appear overly rigid, pushing investors towards countries with more flexible policies. This trend risks positioning the EU as a technology importer rather than a leader, reducing its influence over future digital advancements.

Challenges in implementing individuals' rights

A core aspect of the GDPR is granting individuals rights over their data, such as the right to be forgotten, data portability, and consent withdrawal. While these rights aim to enhance control over one's data, implementing them presents significant challenges for organisations, especially those with decentralised and extensive data systems. The technical and operational difficulties associated with these rights may raise questions about the practicality and proportionality of the GDPR's requirements.

The right to be forgotten requires administrators to delete a user's data, upon request, from all systems and databases. However, executing this right is complex, especially for companies operating in data-intensive sectors or reliant on extensive backup systems. Since their data is often stored in multiple locations – including legacy systems, third-party storage, and cloud environments – complete data erasure is more technically challenging for them. The added obligation to track and remove data from third-party systems further complicates compliance and increases costs.

The right to data portability allows individuals to request their data in a structured, machine-readable format for transfer to another service provider, but this imposes significant technical demands. Implementing data portability requires standardised data formats and compatibility with external systems, which can be resource-intensive, particularly for smaller firms lacking technical infrastructure. In sectors such as healthcare or finance, data portability also poses risks to data integrity and security, as transferring sensitive data increases the risk of breaches.

Consent withdrawal adds another layer of complexity, as the GDPR mandates that users can revoke consent at any time, requiring organisations to cease processing and delete data collected under that consent. This can disrupt ongoing business operations, particularly in sectors dependent on continuous data processing, such as retail trade and advertising where

effective user profiling may provide companies with a competitive edge. Ensuring data removal across interconnected systems is both costly and technically demanding. Additionally, organisations must inform the third parties that received shared data, adding to administrative burdens and increasing the risk of non-compliance.

The GDPR's transparency requirements further compound the compliance burden by mandating detailed and accessible privacy notices. Many organisations find it challenging to balance user-friendly policies with the regulation's comprehensive disclosure obligations. Privacy notices often become lengthy and legally complex, potentially failing to enhance user understanding, contrary to the GDPR's goal of transparency.

Digital Services Act

By Piotr Oliński (FOR)

It would be a trivial remark to state that social media has changed the way European societies function. According to Eurostat, 59 per cent of EU individuals were using social networks in 2023.19 Among businesses, the figure was 60.9 per cent.20 With phenomena such as fake news, the creation of online 'bubbles', and social media's use of data in election campaigns, concern about the impact of social media on democracy and western political systems has grown In the past decade. Concerns have also been raised about the possibility of 'private censorship' by online platforms such as Facebook and Twitter (Fukuyama 2021: 38-40). Some scholars have argued that social media companies have evolved into 'quasi-state actors' with de facto monopolistic and coercive powers (Kim and Telman 2015: 48).

The changes in the digital world were increasingly addressed by court and national legislators. As the European Court of Human Rights pointed out in a Turkish case concerning the blocking of access to YouTube, 'The Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest'.21 Among several legislative initiatives in the EU member states, Germany's NetzDG Act is worth noting.

19 'Nearly 40% of EU's total land area is used for agriculture', Eurostat News, 19 March 2024 (https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240319-1).

20 'Social media - statistics on the use by enterprises', Eurostat Statistics Explained, 30 October 2024 (https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Social_media_-_statistics_on_the_use_by_enterprises).

21 Judgement of the European Court of Human Rights 1 December 2015, Cengiz and Others v. Turkey, §§ 49 and 52.

The act – which obliged large social networks with at least two million users in Germany to immediately delete unlawful content – was presented by the government as a necessary means to combat hate speech and disinformation online. Meanwhile, its critics have pointed out the risks of over-blocking, which include setting limits on freedom of speech and the risk of creating a chilling effect among users (Zurth 2021: 1128-1132). Moreover, NetzDG critics note that the solutions adopted by Germany have been copied by illiberal dictatorships – e.g., Russia and Venezuela – to silence the opposition and those critical of the government online (Mchangama and Fiss 2019).

However, it should be noted that findings from the initial years of the law's application suggest that a minority of content submissions resulted in blocking (Zurth 2021). A similar act, obliging social media platforms to instantly remove hateful content, was introduced in France in 2019, but it was challenged by France's constitutional court as a disproportionate restriction on the right to free expression a year later (see: Mchangama and Alkiviadou 2020).

Motivations behind the Digital Services Act

In 2019, creating 'a Europe fit for the Digital Age' – including the enactment of a new digital services act – was one of Ursula von der Leyen's key goals as a candidate for president of the Commission (Von der Leyen 2019,). Two resolutions of the European Parliament regarding the Digital Services Act (DSA) were adopted in October 2020. Another important context for the DSA is the Commission's European Democracy Action Plan released in December 2020, in which the DSA was intended to play a critical role in countering disinformation (European Commission 2020c).

The DSA was finally proposed as part of a digital package, which included the Digital Markets Act (DMA – see below), in December 2020. Among the objectives of the DSA's 2020 regulatory proposal were:

- ensuring the best conditions for the provision of innovative digital services in the internal market
- contributing to online safety and the protection of fundamental rights
- setting a robust and durable governance structure for the effective supervision of providers of intermediary services (European Commission 2020b)

In the same document, the Commission also noted that member states' increasing legislative activity in the social media domain influences the internal market negatively. It acknowledged the consequent need for harmonisation of laws at the EU level as well as the obsolescence of the previously applicable E-commerce Directive.

From the outset, the EU officials' announcements regarding the DMA were ambitious. Quoting the former Commissioner for Internal Market, Thierry Breton, the act is an attempt 'to organize the digital space for the next decades'.[22] Given the earlier reception of the so-called NetzDG in Germany (see the discussion above) one can venture the thesis that the DSA will have a long-term impact not only in the EU but also in other economies, that are tied to the EU by strong commercial or informational bonds. While it is fair to agree that statements about the EU's 'digital constitution' are a slightly exaggerated description of reality (Wilman 2022: 1), the DSA certainly represents a very significant change in the law and significantly affects the operation of social media and, potentially, the level of freedom of expression online.

Digital Services Act: New obligations on online platforms

The scope of the DSA covers a range of digital entities – such as information society services; intermediary services, including hosting services; online platforms; and online search engines – imposing different responsibilities on each. These responsibilities increase depending on the size and significance of the entity in focus. While information society services of mere conduct face the least obligations – mostly of an informational nature – it is the 'very large' online platforms (VLOPs) and search engines (VLOSEs) that have to bear the greatest regulatory burden.

22 'Digital decade: Commission proposals to make the next 10 years Europe's digital decade', European Commission Press Corner, 15 December 2020 (https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2347).

All intermediary service providers are obligated to do the following:

- designate single points of contact with the competent authorities as well as the recipients
- appoint a legal or natural person as their legal representative in the EU
- include information about any restrictions they impose on recipients in their terms and conditions
- publish a yearly report on content moderation

Hosting service providers have to follow the same requirements and additionally:

- establish mechanisms that allow the users to notify potentially illegal content
- provide a clear and specific ‘statement of reason’ when they impose restrictions on some kind of content
- inform law enforcement or judicial authorities whenever they notice content that might indicate criminal activity or pose a threat to the life or safety of a person/persons

Online platform providers have to comply with all of the above and face additional obligations such as:

- establishing an internal complaint-handling system
- ensuring the possibility of out-of-court dispute settlement
- prioritising notices reported by the so-called ‘trusted flaggers’,
- who are designated by the national coordinator in every member state
- suspend users who frequently post illegal content
- implement appropriate and proportionate measures to protect minors
- bearing other obligations regarding transparency, design, and advertisement

According to the DSA, VLOPs and VLOSEs are platforms with at least 45 million monthly active users on average and have been designated as such by a decision of the Commission. This category of entities must reckon with all of the aforementioned burdens that apply to providers of intermediary services, hosting services, and online platforms and several additional obligations. Among these obligations are:

- conducting a risk analysis for the EU resulting from the operation of their services
- designing measures to mitigate those risks
- haring data with the Commission and cooperating within the framework of the crisis response mechanism
- being subjected to an independent audit at least once a year
- additional transparency, data, and compliance obligations

Initial experiences with the enforcement of the Digital Services Act

The DSA is still a nascent piece of legislation – it only came into full force on 17 February 2024. This makes us still dispose of relatively little material for evaluation, including a lack of case law from the Court of Justice of the EU (CJEU). On 25 April 2024, the Commission announced a list of 17 entities designated as VLOPs, including Amazon Store, Alibaba, Apple AppStore, Facebook, Google Shopping, Instagram, LinkedIn, Twitter (now, X), and TikTok. Simultaneously, it designated Google and Bing as two of the VLOSEs.[23] According to the DSA Enforcement Tracker by think-tank The Future of Free Speech, as of 28 October 2024, 58 investigations had been launched against platforms – all with VLOP or VLOSE status. The vast majority of these cases are at the request-for-information stage.[24]

Two of these cases are noteworthy. The first is that of Amazon Shopping, which challenged its designation as a VLOP in 2023. Similar steps were taken by the German e-retail platform Zalando. The case is pending before the CJEU (case number T-367/23) and will certainly impact the effectiveness of the DSA because it represents a test on how stringent the new

23 'European Commission launches new initiatives to support the EU's digital transition', European Commission Press Corner, 3 May 2020 (https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413).

24 'DSA enforcement tracker', The Future of Free Speech, 30 November 2023 (https://futurefreespeech.org/tracker-of-dsa-enforcement/).

requirements are. Secondly, in December 2023, the Commission opened a formal proceeding against X.[25] In July 2024, X was preliminarily found to be in violation of the DSA regulations. The non-compliance allegations levelled against it focused on the issues of misleadingly marking accounts as verified (granting them blue checkmarks), lack of transparency in advertising, and failure to enable researchers access to public data under the terms outlined in the DSA.[26] Interestingly, in August 2024, Breton published a letter on the X platform – according to press sources, without consulting the Commission president[27] – reminding Elon Musk of his ongoing investigation and obligations under the DSA in the context of a broadcast conversation he was to have with Donald Trump on X. Breton's letter has been widely criticised, among other things, as a threat to free speech[28] and an attempt to interfere in American politics.[29] Indeed, one must agree that this was a dangerous attempt to politicise the DSA and should have been avoided. Such incidents should prompt greater sensitivity to the threats to free speech that could potentially arise from the implementation of the DSA if the EU officials began to misuse it.

Policy recommendations

With legislation such as the DSA come the inevitable risks of instrumentalization and arbitrary application. These risks are made all the more dangerous by the fact that the DSA concerns those forms of freedom that are fundamental to democratic order, such as freedom of speech. Lawmakers, who adopt legislation and regulate its application, should exercise extreme caution and strictness when it comes to the DSA. In our opinion, this legislation still has plenty of room for improvement in this aspect. With this in mind, we recommend:

25 'Commission designates six gatekeepers under the Digital Markets Act', European Commission Press Corner, 11 December 2023 (https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709).

26 'Commission publishes first DSA transparency reports', European Commission Press Corner, 27 May 2024 (https://ec.europa.eu/commission/presscorner/detail/en/ip_24_3761).

27 'EU warns Elon Musk over Trump interview and social media content', Politico, 16 May 2024 (https://www.politico.eu/article/eu-elon-musk-donald-trump-interview-thierry-breton-letter-social-media/).

28 'Open letter to Thierry Breton on the DSA's threats to free speech', The Future of Free Speech, 21 August 2024 (https://futurefreespeech.org/open-letter-to-thierry-breton-on-the-dsas-threats-to-free-speech/).

29 'EU warns Elon Musk over Trump interview and social media content', Politico, 16 May 2024 (https://www.politico.eu/article/eu-elon-musk-donald-trump-interview-thierry-breton-letter-social-media/).

- **Specifying the issue of 'illegal content' further:** The concept of 'illegal content' is central to the application of the DSA. For example, Article 23 requires providers of online platforms to suspend 'recipients of the service that frequently provide manifestly illegal content'. An expansive interpretation of 'illegality' would lead to the notorious social media phenomenon of over-blocking.[30] Just as the guidelines for VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes that were circulated in April 2024,[31] this clarification could initially come in the form of guidelines promulgated by the Commission, explicitly pointing out how over-blocking contradicts the DSA, which prohibits illegal content. Ultimately, consideration could be given to clarifying the riskiest provisions in this regard – such as the aforementioned Article 23 – and perhaps expanding the definition of 'illegal content'. This should be done in line with future CJEU case law.
- **Adopting a human rights–based approach to blocking content:** The proposal to take international human rights law into account has been considered by researchers previously (Mchangama et al. 2022). Such an approach would foster legal certainty by referring to the standard derived from current jurisprudence and could be followed by the Commission both in specific proceedings and in soft-law documents clarifying the provisions of the DSA.
- **Refraining from any attempt to use the DSA politically:** This recommendation does not require extensive elaboration. Freedom, including freedom of expression, is possible under the rule of law and stands contrary to the arbitrary and instrumental application of the law. The EU officials should avoid actions that raise suspicions against such use of the DSA.
- **Considering the creation of an independent digital economy unit:** As proposed by Wörsdörfer (2023) among others, the risks of politicisation could be remedied by the establishment of an independent digital markets unit responsible for enforcement of the DMA, DSA, as well as other acts relating to the digital economy.

30 See Mchangama and Callesen (2022), whose research shows that relatively small amounts of blocked 'hateful' content on Facebook are indeed illegal content.

31 'Guidelines for providers of VLOPs and VLOSEs on mitigation of systemic risks in electoral processes', European Commission Digital Strategy, 26 April 2024 (https://digital-strategy.ec.europa.eu/en/library/guidelines-providers-vlops-and-vloses-mitigation-systemic-risks-electoral-processes).

- **Reviewing the transparency obligations:** Some authors (Barczentewicz 2021) have expressed concerns about the excessive reporting obligations imposed on intermediary services and their negative impact on innovation. The Commission should review them for proportionality after a few years of the DSA's enforcement.

Digital Markets Act: The theoretical background

By Giuseppe Colangelo (Università della Basilicata and IBL)[32]

Motivations and limitations of the Digital Markets Act: Reality versus storytelling

As in any hypothesis of regulatory intervention, the search for the reasons justifying the DMA must necessarily start from an alleged market failure, i.e., from the impossibility of relying on the normal dynamics of competitive forces and on the set of rules traditionally designed to pursue conduct outside the normal competitive game. In this respect, from the outset, the DMA shows rather peculiar traits. Although its application concerns a subset of companies – labelled 'gatekeepers' and, essentially, identified by their size – the real target of the cure is competition law. This law is often accused of being ineffective in the context of digital markets. In this sense, the recitals of the DMA are a veritable cahier de doléance (transl. 'ledger of complaints') about the excessive slowness and complexity of antitrust proceedings compared to the hyper-acceleration of the digital age. Therefore, instead of going through laborious reconstructions of economic analysis, the DMA simplifies the process of investigating market conduct by eliminating any evidentiary burden. That is, we do not need to define the relevant market, ascertain dominance, verify the existence of anticompetitive effects, and assess any procompetitive benefits. Instead, we can rely on a framework built around a long list of absolute obligations and prohibitions.

32 A previous version of this chapter was published in Sileoni, S. and Stagnaro, C. (eds.) (2024) Le sfide delle politiche digitali in Europa. Torino: IBL Libri.

In short, the failure that the DMA aims to address is not that of the market but that of antitrust enforcement. It follows that the DMA takes on the contours of an atypical regulation, as it is a shortcut to enforcing the same conduct that can already be reviewed under traditional competition rules. Further and final confirmation in this sense is plastically offered by the conduct captured in the prohibitions and obligations imposed on the gatekeeper platforms. The list contained in the DMA is, in fact, a collection of investigations performed or initiated by the European and national-level antitrust authorities, so precise that it is easy to associate each provision with the exact procedure (Colangelo, 2023).

Compared to the aforementioned objective, everything appears secondary and marginal in the development of the regulatory intervention in question. In other words, stripped of the list of absolute obligations and prohibitions, there is frankly little left of the DMA. Notwithstanding some references to basic notions in the economic literature on platforms – such as network effects and multi-homing 33– the DMA's approach does not appear to be particularly influenced by them. Moreover, the platforms to which it applies are presumptively designated on the basis of purely quantitative and, therefore, dimensional criteria. This leaves room for qualitative evaluations in the sole, and arduous, forum of contestation of the presumption. The same applies to the legal interests protected. Moreover, the real nature of the DMA is further made explicit also by the reference to principles/ concepts such as fairness and contestability of markets, which traditionally fall within the scope of antitrust rules.

Quite apart from considerations on the appropriateness of introducing a regulation whose sole objective is to facilitate the implementation of certain obligations and prohibitions by eliminating standards and burdens of proof, the comparison with competition law to which the DMA forces us to make leads one to question the actual inability of antitrust laws and practice to cope with the dynamics of digital markets. Indeed, the DMA is the European culmination of widespread and growing dissatisfaction with the application of competition law in all jurisdictions. This criticism essentially revolves around certain pillars such as the slowness of proceedings, an excessive permissiveness favoured by an economic analysis focused exclusively on efficiency-seeking assessments, and the inability, or lack of determination, to impose effective remedies. These factors – and, therefore, what is

33 See Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L 265/1, Recitals 2, 13, 25, 27, 32, 40, 59, 64, and Article 3.

considered an overall and generalised ‘underenforcement’ of antitrust rules – are blamed for allowing a dangerous concentration of power in the hands of a few digital platforms. Conversely, regulation or the profound transformation of competition law are identified as necessary remedies to counter the aforementioned ‘bigness’ of a few operators.

Why the DMA relies on shallow foundations

First of all, references to the investigative and procedural length of antitrust proceedings are exhausted in a single example constantly referred to in support of the thesis, namely the Google Shopping case.34 Decided by the Commission in 2017 after an investigation lasting some seven years, the final word of the CJEU on the matter has been delivered only in late 2024.35 However, this is a classic example that proves too much, as Google Shopping is an outlier. One only has to look at all the other antitrust investigations launched across the EU against digital platforms to realise that the average duration of proceedings is around two years. This is an appropriate and necessary timeframe for due investigations and assessments, which are often complex because conduct in digital markets is often associated with ambiguous effects (Cappai and Colangelo, 2021). Indeed, in markets with two or more sides, the intermediary role of platforms between different groups of users entails that conduct may favour one side rather than another or may be essential to the economic survival of the platform and its business model. Moreover, the same conduct is bound to produce different effects depending on the business model adopted by the platforms.

To this complexity, as mentioned, the DMA responds with detailed and absolute obligations and prohibitions that do not admit of proof to the contrary. Further, they apply indiscriminately to all platforms of a certain size, regardless of the underlying business model. The savings in investigation time are obvious, but this time is saved by dispensing with the investigation itself – in a manner that is close to summary justice – which can end up penalising even conduct that, in a given scenario, may produce benefits for competition. And to be fair, even with the immediacy of DMA enforcement, some perplexity is beginning to emerge: the Commission has already initiated several proceedings for failure to comply with the provisions of the DMA (Colangelo and Ribera Martinez, 2024).

34 European Commission, 27 June 2017, Case AT.39740, *Google Search (shopping)*
35 CJEU, 10 September 2024, Case C-48/22 P.

This suggests that legal disputes do not represent a bothersome feature of competition law but rather a physiological and necessary element for the correct application of the law in general.

Let us turn to the second charge against competition law, namely the alleged underenforcement due to blind submission to the purely efficiency-focused criteria of the consumer welfare of the Chicago school. In the renewed context of the digital age, the idea of promoting a holistic approach that requires competition law to be combined with other areas of law to take into account broad societal interests and ethical goals – such as labour protection, privacy, inequality, and sustainability – thus re-emerges. Since addressing the eternal revival of the debate on the objectives and true soul of antitrust law is not within the scope of this work, we will instead discuss the reported failure of antitrust enforcement. On balance, i.e., by examining the proceedings initiated against digital platforms, the numbers do not seem to support this thesis. Moreover, the DMA, as has been pointed out, is a photographic compilation of previous antitrust proceedings, almost all of which were successfully concluded for competition authorities, including, in some cases, the Commission itself (Colangelo, 2023).

It remains to address the third issue, that of the effectiveness of remedies. This aspect seems to be the most relevant and, at the same time, the most difficult to address. While the rules and theories of harm in antitrust law remain flexible enough to handle even the alleged and real peculiarities of digital markets, the definition and implementation of remedies is undoubtedly a delicate and controversial step that tests the limits of competition law. This is essentially related to the economic peculiarities of digital markets and the inherent ambiguity of many strategies implemented in two-sided markets (Cappai and Colangelo, 2021). It follows that the scope of remedies may affect the design of products/services and/or the business model of the platform, if not even the structure of the company. Both hypotheses raise complex issues, sometimes requiring one to deal with highly technical aspects or assess possible negative consequences in terms of innovation.

The Android Auto case, currently before the CJEU, provides an emblematic example of what appears to be the Herculean columns of antitrust law.[36] The case stems from an Italian dispute between the electricity and EV charge supplier Enel and Google over the latter's refusal to ensure the

36 CJEU, Case C-233/23, Alphabet et al v. Autorità Garante della Concorrenza e del Mercato.

interoperability of the JuicePass app with Android Auto.37 Quite apart from the reasons put forward by Google, the Italian antitrust authorities suspect that behind the refusal is Google's interest in protecting its own Google Maps app from potential competition from a rival product that would allow users to track down charging stations for electric cars as well as to book and pay for the service in advance. As a result, the antitrust authority sanctioned Google and required it to develop a 'template' that would allow all developers of apps similar to Enel's to be available on Android Auto.

However, the peculiarities of the case and, in particular, of the remedy imposed led the Italian administrative judges to seek clarification from the CJEU. Leaving aside the relevant and potentially decisive legal question of the essential nature of the infrastructure in question (Android Auto), it is, for our purposes, particularly interesting to focus on the ancillary questions submitted to the CJEU. Specifically, the Italian administrative courts ask whether the antitrust rules must be interpreted as meaning that:

> (i) the non-existence of the product/service at the time of the request for supply must be taken as an objective justification for refusal or, at the very least, whether a competition authority is obliged to perform an analysis of the time needed by a dominant undertaking to develop the product/service for which access is requested
>
> (ii) a dominant undertaking that controls a digital platform can be required to modify its products or develop new products, to provide access to those products to requesters and, if so, whether the undertaking must consider the general needs of the market or the specific needs of the individual requesting access.[38]

Far from trying to anticipate the CJEU's answers, the questions in any case point to the enormous difficulties encountered in managing, with the traditional tools of competition law, a remedy prescribing interoperability in digital environments. Once a request for access has been granted, clear indications must be provided on the economic aspects and, above all, on the technical modalities. Failure to do so risks creating an ineffective

37 Italian Competition Authority, 27 April 2021, Decision No. 29645, *Google/Enel X*.
38 Consiglio di Stato, 7 April 2023, No. 3584, Alphabet et al v. Autorità Garante della Concorrenza e del Mercato.

remedy, as the company being subjected to the interoperability obligation may enforce practices that undermine the objective and prevent rivals from competing on equal terms. On the contrary, regulation is better equipped, at least in theory. This is mainly because regulators are familiar with defining and supervising conditions and terms of access to infrastructure.

If these are the prerequisites, it is evident that the enactment of the DMA has raised considerable expectations as to the possibility of bridging the above-mentioned gap by identifying and imposing effective remedies to promote competition in digital markets, e.g., through interoperability obligations. In other words, it is to be expected that a dispute such as the Android Auto could be handled more easily and quickly in the aftermath of the DMA, given that the latter includes several horizontal and vertical interoperability obligations. These obligations include a specific one pursuant to which gatekeepers are obliged to ensure, free of charge, effective interoperability – and access for interoperability purposes – with the same operating system and hardware or software components that are available or used in the provision of its complementary and support services and hardware (Article 6.7).

What could possibly go wrong?

Even in this case, there is a real risk that enthusiasm and expectations will cool.

With the regulatory approach, the burden of intervention and proof is no longer on the antitrust authority. It is, instead, the addressee companies that have to demonstrate how the proposed changes in their business models for DMA compliance are actually in line with the letter and spirit of the new rules. However, despite the proclaimed clarity and even self-enforceability of the DMA rules, it does not appear that the DMA obligations are so easy to apply and enforce. This is particularly evident when compliance involves strategic decisions regarding the design of the technical features that may either address genuine security and privacy concerns or be exploited to undermine potential competition. These different scenarios are extremely difficult to navigate for the authorities.

In this scenario, under the DMA, the Commission can activate different types of procedures – from regulatory dialogue to punitive interventions – to compel gatekeepers to ensure effective enforcement. However, the Commission does not have the power to determine what exactly compliance

should be. It could, therefore, be said that the DMA does not allow the regulator to regulate fully because it cannot actively provide operators with precise guidance on how to comply with the new rules. The Commission's initiation of numerous non-compliance proceedings seems to confirm that litigation will also be a practice in the enforcement context of the DMA, thus replicating the traditional and much-reviled antitrust enforcement dynamics.

In the face of questionable ideas underlying the DMA, uncertain advantages, and apparent limitations of the DMA, significant counterproductive effects emerge, first and foremost, concerning the tricky and dangerous cohabitation between regulatory measures and competition law. As mentioned, the DMA draws inspiration from antitrust investigations by crystallising in prohibitions 'per se' conduct that is already under the purview of competition law. As if this were not enough, the stated legal interests protected by the DMA – 'fairness' and contestability of markets – are not peculiar to those already protected by competition law.

Finally, the DMA justifies itself by comparison with the alleged limits of antitrust law in terms of the type of intervention – ex-ante versus ex-post; the scope of application – gatekeeper versus dominant firms; and the standard of analysis – absolute prohibitions versus economic analysis. And yet, the DMA does not replace competition law but presents, at least in the wishes of its promoters, a complement to it. This gives rise to the following side effects.

First of all, there is an alteration of the traditional balance between regulation and competition. To be fair, the boundaries between antitrust laws and regulation have always been fluid. After all, the interaction between these two domains of legislation has gone through various phases, moving from rivalry to complementarity. This is mainly because the very concepts of antitrust and regulation have long been debated. However, over time, the literature has managed to converge on a number of shared conclusions that are summarized below.

Apart from the debated questions on the ultimate goals of antitrust, competition is commonly accepted as the best regulator, which means that effective antitrust policy reduces the need for regulation. Indeed, effective competition leads to lower prices, better quality for existing products and services, and innovation in new products and services. To this end, antitrust laws address market power through a flexible and

horizontal system of restrictions typically applied retrospectively. In this sense, they perform a prophylactic function by safeguarding the competitive process rather than dictating market outcomes. In contrast, regulation is prescriptive. It favours intervention based on a rigid set of clear – and, usually, sector-specific – rules whereby the required conduct is identified from the outset. As a result, regulation is more effective in addressing competition problems that arise from structural market imperfections.

It follows that the discriminant between antitrust and regulation is the presence of a market failure. Therefore, outside the discussed hypothesis, economic regulation should leave as much room as possible for competition law. Furthermore, according to the principle of proportionality, regulators should refrain from introducing artificial barriers to entry, such as high administrative and compliance costs. Similarly, regulation should be transitional in time and scope and as flexible as possible, especially when dynamic markets are involved. For the reasons already outlined, the DMA does not fit into this category (see, for example, Stagnaro and Turillazzi, 2022).

Forcing the traditional relationship between antitrust and regulation has, however, led to an even more significant counterproductive effect. To avoid fragmentation of the internal market, the DMA contains a provision that prevents member states from imposing further obligations on gatekeepers vis-à-vis measures ensuring fairness and contestability of digital markets, thus addressing regulation and not competition law. However, nothing prevents the member states from updating and strengthening their national antitrust regulations with reference to digital platforms. Following the DMA's enforcement, some member states have started an arms race, endowing their national antitrust authorities with new powers, such as new rules on the abuse of economic dependence, market investigation, and the introduction of presumptions in the assessment of the most recurrent practices in digital markets (Colangelo, 2024). Therefore, some member states have enacted a kind of national mini-DMA by introducing instruments that rival the DMA in terms of enforcement shortcuts. This allows national-level antitrust authorities to compete with the Commission for the role of digital market enforcer.

The overlap between the DMA and competition law enforcement has a twofold implication. On the one hand, companies are exposed to the real risk of being prosecuted for the same conduct on the basis of both the DMA and the old and new antitrust provisions, in clear violation of the ne

bis in idem principle. On the other hand, the European Single Market is also threatened by such regulatory fragmentation. The DMA's justification for harmonisation at the European level is the cross-border nature of services provided by digital platforms, which often deploy their business models globally, thus making it impossible for member states acting alone to effectively address the identified competition problems. The DMA explicitly states that the application of national rules may undermine the functioning of the Single Market for digital services and the functioning of digital markets in general (see Recitals 7 and 9). It is clear, however, that the scenarios of overlapping and dual application of the DMA and national antitrust provisions just outlined demonstrate that, in the post-DMA world, the European regulatory landscape will be even more fragmented.

The damage done to the laborious and still incomplete construction of the internal market is not matched by any particular success in the promotional campaign launched to export the European vision abroad, under the flag of making the EU a "regulatory superpower" (see, for example, Šonková 2024). One of the objectives pursued by the European institutions through the DMA and the numerous further legislative initiatives in the digital sphere is to promote the so-called 'Brussels effect', i.e., to assert European leadership as a regulatory model for other countries. While it may make sense to claim primacy in the production of standards – in principle, innovation does not come through regulation, which is often the main brake – the results of this competition do not currently reflect the propaganda. Indeed, there are not many countries in the world that have decided to follow in European footsteps. Some of them have taken their cue from the European experience to design digital market regulation models antithetical to the DMA, for example, the UK and Australia (Colangelo, 2023). Others, notably the US, do not seem close to changing their current competition rules.

To sum up, if the DMA's mission to stand as a beacon for the regulation of digital markets appears to have failed at the moment, the acclaimed Brussels effect does not seem to be felt in Europe either since several member states have shirked the attempt at harmonisation and centralised application of the DMA.

Digital Markets Act: How to improve it

By Piotr Oliński (FOR)

Market power and free societies in the digital era

Digital Markets Act: Overview of solutions.

The DMA was proposed to address a key problem of the previous proceedings initiated under Article 102 of the Treaty on the Functioning of the European Union (TFEU) – their slow pace and reactivity (Monti 2021). The addressees of the Act's obligations are so-called gatekeepers, i.e., entities that i) have a significant impact on the internal market, ii) provide a core platform service that is an important gateway for business users to reach the end users, and iii) enjoy an entrenched and durable position in their operations or it is foreseeable that they will enjoy such a position in the near future (Art. 3, point 1. DMA). The list of gatekeepers is reviewed once at least every three years. At present, there are six designated gatekeepers: Alphabet, Amazon, Apple, ByteDance, Meta, and Microsoft.39. These include:

- combining, cross-using or processing the personal data of platform users without their consent
- preventing business users from offering the same products or services on their own or third-party websites
- blocking or charging the communication and promotions of offers between business users and consumers through other channels

39 'Gatekeepers', European Commission, 8 September 2024 (https://digital-markets-act.ec.europa.eu/gatekeepers_en).

- blocking end users' access to content, features, or subscriptions acquired without using the core platform
- preventing or restricting business users or end users from raising issues of the gatekeeper's non-compliance with the relevant Union or national laws with any relevant public authorities
- requiring end users or business users to use a particular search engine or payment service
- requiring end users or business users to subscribe to further core platform services

The gatekeeper is also obliged to inform the Commission of planned concentrations and submit an independently audited description of the user profiling techniques used to the Commission.

The DMA constitutes an ex-ante regulation, promoting complementary but not identical objectives to EU competition law (Monti 2021). At the same time, its application is without prejudice to the application of Articles 101 and 102 TFEU (Article 1(6) DMA). In short, the relationship between EU competition law and the DMA can be described as a lex specialis intended to facilitate the Commission's proceedings, as is the case with the relationship between competition law and regulation in the energy or telecommunications sector (Monti 2021).

Policy recommendations

The DMA is still a fresh piece of legislation; suffice it to say that the Commission's first annual report on it has only just been published. It, therefore, seems far too early to prejudge its effectiveness or otherwise. However, it is worth drawing the new Commission's attention to the directions in which it would be worthwhile to develop the current legislation if reform were to be attempted.

- **Independent digital economy enforcer:** Currently, the Commission, which is both an administrative and a political body, is responsible for enforcing the DMA. This situation may raise doubts about the independence of the enforcement of the DMA. It should be noted that this remark applies to both the DSA and classic competition law at the EU level. In the long term, the establishment of a separate and independent digital markets unit responsible for the application of the

DMA and DSA seems worthy of consideration, as also suggested by Wörsdörfer (2023).

- **Private enforcement:** The Commission should monitor the private enforcement of the DMA since it has the potential to complement the administrative measures taken by the Commission and national authorities (Wörsdörfer 2023). Should this scope prove to be extremely modest, provisions explicitly addressing private enforcement in the DMA could be considered.
- **Merger control:** The obligations that the DMA imposes on mergers are extremely weak. For instance, gatekeepers need only notify the Commission in this regard. Juxtaposed with tendencies to loosen the merger control regime under traditional competition law – as reflected, for example, in the Draghi report's 'innovation defence' proposal (Draghi, 2024: 299) – this risks ineffective control of mergers and acquisitions in the digital economy. This challenge does not necessarily have to be answered by the DMA. Consideration could be given, for example, to merger control reform, as called for by the Bundeskartellamt, the British Competition and Markets Authority, and the Australian Competition and Consumer Commission (Wörsdörfer 2023).
- **Towards structural remedies:** Should the DMA prove marginally effective, there remains plenty of room for structural remedy reforms. One possible change would be to adopt a solution familiar to, say, the regulation of the energy sector. Similarly, some form of unbundling of related platform services could be proposed.

The EU's AI regulations: Fostering innovation and upholding freedom of expression

By Diana Năsulea (IES-Europe) & William Hongsong Wang (Fundalib)

The European Union has solidified its reputation as a global regulatory powerhouse with the enactment of its Artificial Intelligence Act, completing a legislative triad alongside the Digital Markets Act and the Digital Services Act. Hailed as a harmonizing framework for AI rules across member states, the AI Act was adopted by the European Parliament on March 13, 2024, approved by the EU Council on May 21, 2024, and enacted on August 1, 2024. The regulations will take effect in stages with varying implementation timelines. While the act has been lauded for its consumer protections and democratic safeguards, critics warn that the EU's fine-grained approach, while well-intentioned, risks undermining innovation and long-term societal welfare40. As the world's largest regulatory body ventures further into the digital sphere, the tension between regulation and technological progress comes sharply into focus.

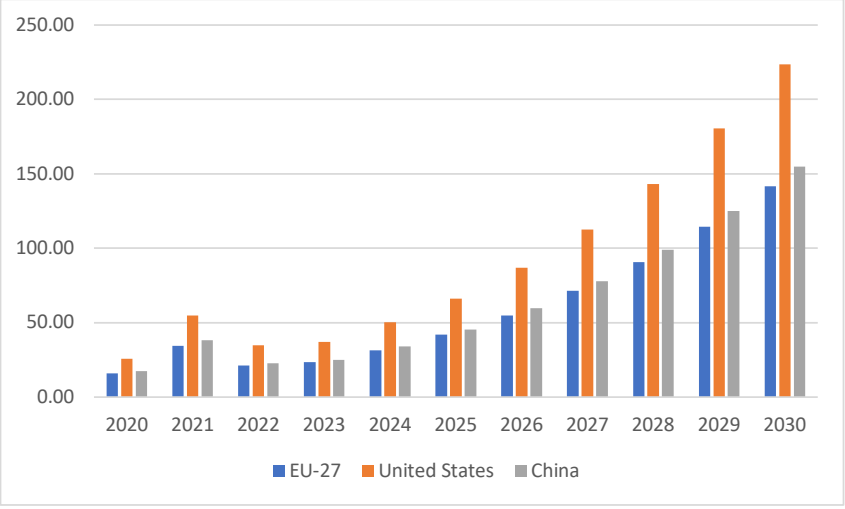
The Competitive Challenge in AI Investment

When it comes to the competitive advantage of the EU, the economic trends highlight the EU's lag in AI investment and development compared to global competitors. Data from 2020 to 2030 show that while the EU-27

40 Varad Raigonkar, ` European Union's AI Law Will Heavily Regulate a Technology Lawmakers Don't Understand`, Reason, 22 March 2024, https://reason.com/2024/03/22/european-unions-ai-law-will-heavily-regulate-a-technology-lawmakers-dont-understand/

is steadily increasing its AI investments, it significantly trails behind the United States and China. For instance, in 2025, the EU's AI investment is projected to reach €41.83 billion, compared to €66.21 billion in the United States and €45.45 billion in China. This gap widens further by 2030, with the EU's investment at €141.80 billion, dwarfed by the United States at €223.70 billion and China at €154.80 billion. The slower growth in AI funding underscores the challenges posed by stringent regulatory measures, which may discourage private sector engagement and innovation, placing the EU at a competitive disadvantage in the global AI race. To use the words of Anand Sanwal, CEO of CB insights, "The EU now has more AI regulations than meaningful AI companies"41.

Fig 1. AI Market Size in EU-27, USA and China - Projection



Source: Statista, Artificial Intelligence - EU-27, United States, China. (n.d.)

Balancing Innovation and Regulation: The European Union's AI Act

The rapid advancement of artificial intelligence (AI) presents both unprecedented opportunities and significant risks, prompting global policymakers to navigate a delicate balance between fostering innovation and ensuring societal safeguards. In this context, the European Union

41 https://mailchi.mp/a3eba8791064/europe-dont-love-ai?e=0fd180b925

(EU) has positioned itself as a leader in regulating AI through its proposed Artificial Intelligence Act (AI Act). This legislation, touted as the world's first comprehensive legal framework for AI, seeks to mitigate the risks associated with AI while promoting its ethical and responsible deployment. However, its approach has sparked debates about its potential overreach and implications for innovation (Veale & Borgesius, 2021).

The AI Act is designed to address the dual objectives of ensuring safety and alignment with fundamental rights while fostering an environment conducive to innovation42. It introduces a tiered, risk-based framework that categorizes AI applications according to their potential impact. At one extreme, applications deemed to pose "unacceptable risks," such as systems enabling social scoring by governments or real-time biometric surveillance in public spaces, are outright banned. In the intermediate "high-risk" category, systems that impact critical areas such as healthcare, education, law enforcement, and employment are subject to stringent requirements. These include mandatory risk assessments, human oversight, and rigorous testing to ensure compliance with transparency and accountability standards. Lower-risk applications face limited regulatory obligations, reflecting an effort to avoid stifling innovation in areas considered less critical.

Even if it were possible to oversee the entire field of AI—which it is not—the EU would require an intentional definition of AI. This would involve defining the concept by its inherent meaning or characteristics, fostering a deeper theoretical understanding of AI rather than merely listing examples or instances that fall under its scope. Instead, the AI Act offers an extensional definition by categorizing applications into risk levels. This choice highlights the EU's limited grasp of the technology at hand, treating AI more as a product and aligning much of its framework with traditional product safety regulations.

The limitations of this approach become evident when applied to General Purpose AI systems, such as OpenAI's ChatGPT, Meta's Llama, or Google's Gemini. Unlike single-purpose products—like spam filters—whose risks can be assessed and regulated effectively, General Purpose AI systems are versatile and adaptable, serving countless applications. This versatility makes it nearly impossible to assess all potential risks comprehensively or to create regulations that anticipate every conceivable use. Attempting

42 European Commission, AI Act, 2024, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

to regulate such systems at this early stage of their development recalls the hypothetical folly of the Continental Congress in 18th-century North America trying to regulate all uses of electricity. Just as electricity's transformative potential could not have been fully understood or regulated during its infancy, the same holds true for AI[43].

Despite its structured approach, the AI Act has been criticized for its potential to overregulate[44], particularly in the context of emerging and general-purpose AI technologies. For example, large language models and other versatile AI systems are classified as high risk under certain circumstances, even though their applications may span a wide range of low-risk activities. This broad classification risks imposing disproportionate compliance costs on developers, particularly smaller enterprises and startups. A report by the Center for Data Innovation suggests that compliance costs for high-risk AI systems could reach up to €400,000 for a small business with an annual turnover of €10 million, equivalent to approximately 4% of annual revenue[45]. This places a significant financial burden on smaller actors, potentially disincentivizing innovation and market participation. Furthermore, the Centre for European Policy Studies clarified that high compliance costs primarily affect high-risk applications, constituting a relatively small fraction of AI investments, but warned against the misapplication of these estimates to broader AI markets[46]. By contrast, larger corporations with extensive resources are better positioned to absorb these costs, potentially consolidating their dominance in the AI sector.

Additionally, the Act's definitions of key terms such as "high-risk" and "systemic risk" remain ambiguous, leading to uncertainties about how the rules will be applied. For instance, biometric identification technologies used in niche, controlled environments may be subjected to the same rigorous standards as those deployed in public spaces,

43 Henrique Schneider, ` The AI Act: The EU's serial digital overregulation`, GIS, 10 October 2024, https://www.gisreportsonline.com/r/ai-act-eu-regulation-innovation/

44 Henrique Schneider, ` The AI Act: The EU's serial digital overregulation`, GIS, 10 October 2024, https://www.gisreportsonline.com/r/ai-act-eu-regulation-innovation/

45 Benjamin Mueller, `AI Act Would Cost the EU Economy €31 Billion Over 5 Years, and Reduce AI Investments by Almost 20 Percent, New Report Finds`, Center for Data Innovation, 26 July 2021, https://datainnovation.org/2021/07/ai-act-would-cost-the-eu-economy-e31-billion-over-5-years-and-reduce-ai-investments-by-almost-20-percent-new-report-finds/?utm_

46 Moritz Laurer, Andrea Renda, Timothy Yeung, `Clarifying the costs for the EU's AI Act`, CEPS, 21 September 2021, https://www.ceps.eu/clarifying-the-costs-for-the-eus-ai-act/?utm

despite their vastly different risk profiles. Such regulatory ambiguity could discourage investment and experimentation, with some companies opting to relocate to jurisdictions with more flexible frameworks, such as the United States or China, where AI development continues to thrive under less restrictive oversight[47].

The AI Act also aims to “avoid undesirable outcomes” and establish a governance structure at both the European and national levels. This includes the creation of the European AI Office, intended to serve as the central hub for AI expertise within the EU. The law centralizes AI regulation across member states to ensure a harmonized standard—a hallmark of EU regulatory efforts—but also introduces steep penalties for non-compliance. Fines range from €35 million or 7% of global revenue for severe violations to €7.5 million or 1.5% of revenue for lesser infringements, making adherence to the regulation a costly endeavor for companies[48].

Proponents of the AI Act argue that these regulatory measures are necessary to foster trust and ensure the ethical use of AI. They emphasize that public concerns about privacy, discrimination, and the potential misuse of AI necessitate robust safeguards[49]. By mandating transparency and accountability, the legislation aims to build user confidence in AI systems, which is seen as critical for their widespread adoption. Furthermore, the EU’s focus on establishing itself as a global standard-setter for AI regulation is intended to harmonize international governance frameworks, reducing the risks of regulatory fragmentation and fostering a level playing field in global markets.

However, the Act’s heavy-handed approach to regulation may undermine its stated goals. The inclusion of “systemic risks”—a late addition to the legislation—illustrates the difficulties in delineating what constitutes an unacceptable risk. For instance, general-purpose AI systems like ChatGPT, which can be fine-tuned for various applications, are now subject to additional scrutiny under Title VIII-A of the Act[50]. Critics argue that such

47 Javier Espinoza, ` Europe’s rushed attempt to set the rules for AI`, Financial Times, 16 July 2024, https://www.ft.com/content/6cc7847a-2fc5-4df0-b113-a435d6426c81?utm_

48 EU AI Act, Art 99: Penalties https://artificialintelligenceact.eu/article/99/

49 European Commission, AI Act, 2024, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

50 EPRS, General-purpose artificial intelligence, March 2023, https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/745708/EPRS_ATA%282023%29745708_EN.pdf?utm_

measures reflect an overly cautious stance that conflates theoretical risks with practical applications. This could delay the deployment of beneficial AI technologies in critical sectors such as healthcare[51], where AI-driven diagnostic tools have demonstrated the potential to improve patient outcomes significantly.

The regulatory challenges posed by the AI Act underscore the importance of adopting a more flexible, proportionate approach. Simplifying compliance processes for small and medium-sized enterprises (SMEs) could alleviate barriers to innovation while ensuring that necessary safeguards remain in place. The creation of regulatory sandboxes, where developers can test AI systems in controlled environments, offers a promising model for balancing oversight with experimentation. Furthermore, enhancing collaboration between regulators, industry stakeholders, and academic experts could lead to more nuanced policies that reflect the realities of AI development.

The AI Act represents a pioneering effort to govern AI in a manner that seeks to balance innovation with ethical considerations. While its focus on trust, transparency, and safety is commendable, its potential to overregulate and stifle innovation cannot be ignored. By refining its provisions to address these concerns, the EU can position itself as a global leader in shaping the future of AI governance. Achieving this balance will require ongoing dialogue and adaptability, ensuring that the legislation evolves alongside technological advancements while safeguarding fundamental rights and societal values.

Sociological Dimensions of Risk and Regulation

The regulation of AI at the EU level is underpinned by a risk-based approach. Beginning with the *Ethics Guidelines on Trustworthy AI*[52] and the White Paper on AI (European Commission, 2020), European efforts have revolved around identifying and managing risks associated with AI. The draft AI Act introduced a tripartite risk classification—unacceptable, high, and low/minimal risks—establishing distinct regulatory obligations for each category.

---

51 Lisa Falco, Johanna O'Donnell, ` AI regulation in healthcare: will legislation impact innovation?`, 13 December 2023, https://www.zuehlke.com/en/insights/healthcare-regulation-will-ai-legislation-impact-innovation?utm_source=chatgpt.com

52 High-Level Expert Group on AI. 2019. "Ethics Guidelines for Trustworthy AI". Text. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai(open in a new window).

Unacceptable risks, such as social scoring by governments, are banned outright. High-risk systems, like those determining access to education or employment, face stringent requirements, including lifecycle risk management, transparency, data quality controls, human oversight, and conformity assessments.

Notably, the AI Act goes beyond traditional notions of risk—such as those affecting health and safety—to encompass risks to fundamental rights. Annex III of the AI Act identifies systems impacting critical areas like recruitment and education, where the primary concern is the safeguarding of equality and non-discrimination. This broad conceptualization of risk, which includes systemic risks posed by general-purpose AI models, reflects the EU's commitment to aligning technological innovation with human rights and societal values.

However, the expansive nature of the EU's AI regulation also introduces complexities. As Luhmann's systems-theoretical perspective suggests, risk is inherently subjective, shaped by the diverging observations and attributions of various stakeholders (Luhmann, 2005). The AI Act's recognition of risks to public interests and fundamental rights challenges traditional sociological notions of risk, necessitating a nuanced understanding of its communication and attribution. By combining robust regulatory mechanisms with an emphasis on innovation and individual freedoms, the EU's approach aims to strike a delicate balance. Yet, as debates around AI governance evolve, questions remain about whether this risk-based framework can adequately address the rapid pace of technological change without stifling innovation or creating regulatory paradoxes.

In recent years, the intersection of public activism, academic research, and policymaking has increasingly emphasized the risks posed by artificial intelligence (AI). Scholars and activists have highlighted its potential to disrupt individual lives, exacerbate inequalities, and even destabilize democratic institutions (Bender et al., 2021; Burt, 2018; EDRi, 2021). Despite these warnings, AI continues to be framed as both an inevitable force and a critical driver of economic growth (Bareis & Katzenbach, 2022). However, the ethical turn in AI governance, often promoted through science and industry-led guidelines, has been criticized as a means to forestall meaningful legal regulation (Rességuier & Rodrigues, 2020).

The European Union has sought to move beyond ethical platitudes with a regulatory framework exemplified by the AI Act. This legislation,

complemented by other governance instruments, aims to mitigate the risks associated with AI while fostering innovation (Veale, Matus, & Gorwa, 2023). Yet, discussions surrounding the AI Act have largely been confined to its legal merits and shortcomings, leaving its sociological dimensions—particularly those related to the communication of risk—underexplored.

Drawing from Luhmann's systems theory, Kusche (2024) explains that the notion of risk is best understood as a communicative construct, inherently tied to decision-making and the attribution of harm (Luhmann, 2005). This perspective is critical for understanding how AI-related risks are framed and addressed in European policy. According to Luhmann, risk is a product of modernity, replacing earlier notions of fate and divine intervention with uncertainty rooted in human decision-making (Luhmann, 1992). This uncertainty manifests in three communicative dimensions: temporal, factual, and social.

In the temporal dimension, risk reflects the unpredictability of the future as shaped by present decisions. The European Commission's *White Paper on AI* (2020) underscores this dynamic, blending optimism about AI's economic potential with warnings of societal stagnation if AI is not properly adopted and regulated. This dual framing—where AI is both a promise and a threat—illustrates a "future essentialism" (Schiølin, 2020), positioning regulation as an adaptation mechanism.

The factual dimension further complicates the narrative, as the distinction between "risk" (attributed to one's own decisions) and "danger" (attributed to external decisions) becomes blurred. For example, the EU's emphasis on aligning AI development with "EU rules and values" implicitly identifies external actors—such as foreign governments or private companies—as potential sources of danger (European Commission, 2020). This framing situates the EU as a self-regulator in a global environment characterized by divergent value systems.

The social dimension highlights the inherent tension between decision-makers and those affected by their decisions. The EU's regulatory ambition is framed as a means of fostering trust, emphasizing "trustworthy AI" as a central pillar of its approach (European Commission, 2020; High-Level Expert Group on AI, 2019). However, this notion of trustworthiness creates a paradox: the regulation seeks to inspire confidence in AI systems precisely because their potential for harm remains significant.

These communicative dimensions reveal fundamental tensions in how the EU delineates and addresses AI-related risks. While the AI Act aspires to provide legal certainty, its reliance on the concept of risk exposes the limitations of current regulatory frameworks. The Act expands the scope of risk regulation to include fundamental rights and systemic risks, yet it struggles to reconcile these abstractions with concrete, actionable rules. This dissonance underscores the challenges of bridging sociological insights with legal and political decision-making.

Policy Recommendations

The AI Act is a bold step in establishing a comprehensive governance framework for artificial intelligence, reflecting the EU's commitment to ethical standards and societal safeguards. However, the complexities of regulating rapidly evolving technologies and the potential unintended consequences of overregulation highlight the need for refinements. To ensure that the Act fosters innovation while maintaining its core objectives of safety, transparency, and trust, targeted policy interventions can address key challenges. These recommendations aim to strike a better balance, enabling the EU to lead globally in AI governance without hindering technological progress.

1. Regulatory Sandboxes for innovation: Establishing controlled environments for SMEs to test AI systems would allow innovation to thrive without compromising oversight. Such sandboxes can facilitate compliance while reducing barriers for smaller enterprises.

2. Refinement of definitions and risk frameworks: Ambiguous terms such as "high-risk" and "systemic risk" should be clarified to ensure that regulatory requirements are proportionate to the actual risk level of each application. For instance, biometric systems used in controlled, low-risk environments could be subjected to less stringent regulations than those deployed in public spaces. This refinement would prevent overregulation and promote fairness in compliance obligations.

3. Enhanced stakeholder collaboration: Enhanced collaboration among regulators, industry leaders, and academic experts can foster the development of nuanced, adaptive policies that reflect the realities of AI technology. By involving diverse perspectives and expertise, the AI Act can evolve to address emerging challenges and opportunities, ensuring its relevance and effectiveness in a rapidly advancing field.

References

European Commission (2021a) *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Brussels: European Commission.

European Commission (2021b) *Annexes to the proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Brussels: European Commission.

Veale, M. and Borgesius, F. Z. (2021) Demystifying the draft EU Artificial Intelligence Act. *Computer Law Review International* 22(4): 97–112.

Wachter, S., Mittelstadt, B., and Floridi, L. (2021) Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law* 7(2): 76–99.

Barczentewicz, M. (2021) The new European Digital Services Act: Risky for consumers and innovation. Brussels: Epicenter.

Bareis, J., & Katzenbach, C. (2022). Talking AI into being: The narratives and imaginaries of national AI strategies and their performative politics. *Science, Technology, & Human Values, 47*(5), 855–881. https://doi.org/10.1177/01622439211030007.

Baumeister, T. (2022) Section 19a GWB as the German 'Lex GAFA' – lighthouse project or superfluous national solo run? *Yearbook of Antitrust and Regulatory Studies* 15(26): 75–102.

Bender, E. M., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the dangers of stochastic parrots: Can language models be too big? *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 610–623. https://doi.org/10.1145/3442188.3445922.

Bessen, J. E., Impink, S. M., Rerichensperger, L., and Seamans. R. (2020) GDPR and the importance of data to AI startups. NYU Stern School of Business.

Böhm, F. (2010) [1933] *Wettbewerb und Monopolkampf*. Baden-Baden: Nomos.

Burt, A., Leong, B., & Shirrell, S. (2018). *Beyond explainability: A practical guide to managing risk in machine learning models*. Future of Privacy Forum. https://fpf.org/wp-content/uploads/2018/06/Beyond-Explainability.pdf.

Cappai, M., Colangelo, G. (2021). Taming digital gatekeepers: the more regulatory approach to antitrust law, *Computer Law & Security Review* 41: 105559.

Colangelo, G. (20234) Trendy antitrust for digital markets: are market investigations the new black?DMA begins. *Journal of European Competition Law & PracticeAntitrust Enforcement* 115(15): 289116-298122.

Colangelo, G. (2024). Trendy antitrust for digital markets: are market investigations the new black? *Journal of European Competition Law and Practice* 15(5): 289-298.

Colangelo, G., Ribera Martinez, A. (2024). The Metrics of the DMA's Success. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4959671.

Crémer, J., de Montjoye, Y.-A., and Schweitzer, H. (2019) *Competition policy for the digital era. Final report*. Luxembourg: Publications Office of the European Union.

De Streel, A. (2020) Should digital antitrust be ordoliberal? Foreword. *Concurrences* (1): 2–4.

EDRi. (2021). *Beyond debiasing: Regulating AI and its inequalities*. https://edri.org/wp-content/uploads/2021/09/EDRi_Beyond-Debiasing-Report_Online.pdf.

Eucken, W. (2004) [1952] *Grundsatze der Wirtschaftspolitik*. Tubingen: Mohr Siebeck.

European Commission (2020a) *Communication from the Commission to the European Parliament and the Council. Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation COM/2020/264 final*. Brussels: European Commission.

European Commission (2020b) *Explanatory memorandum to the proposal for a regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC*. Brussels: European Commission.

European Commission (2020c) *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions on the European Democracy Action Plan ("European Democracy Action Plan") COM 2020*. Brussels: European Commission.

European Commission (2024a) *Communication from the Commission to the European Parliament and the Council. Second Report on the application of the General Data Protection Regulation COM/2024/357 final*. Brussels: European Commission.

European Commission (2024b) *The future of European competitiveness – A competitiveness strategy for Europe*. Brussels: European Commission.

European Commission. (2020). *White paper on artificial intelligence: A European approach to excellence and trust*. https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

European Parliament (2020) The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. Brussels: European Parliament.

European Union (2016) *Regulation (EU) 2016/679 (General Data Protection Regulation)*. Brussels: European Union.

European Union Agency for Fundamental Rights (2024) *GDPR in practice: Experiences of data protection authorities*. Vienna: European Union Agency for Fundamental Rights.

Floridi, L. (2019) Establishing the rules for building trustworthy AI. *Nature Machine Intelligence* 1(6): 261–2.

Fuest, C., Gros, D., Mengel, P.-L., Presidente, G., and Tirole, J. (2024) Reforming innovation policy to help the EU escape the middle-technology trap. CEPR.

Fukuyama, F. (2021) Making the Internet Safe for Democracy. *Journal of Democracy* 32(2): 37–44.

Goldschmidt, N. and Wohlgemuth, M. (eds.). (2008) *Grundtexte zur Freiburger Tradition der Ordnungsökonomik*. Tübingen: Mohr Siebeck.

High-Level Expert Group on AI. (2019). *Ethics guidelines for trustworthy AI*. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

High-Level Expert Group on Artificial Intelligence (2019) *Ethics guidelines for trustworthy AI*. Brussels: European Commission.

Institut économique Molinari et CroissancePlus (2021) Pour une réforme des retraites qui réponde aux enjeux français - Compétitivité, emploi, innovation avec la capitalisation pour tous. Paris.

Irish Council for Civil Liberties (ICCL). (2021) *Economic and reputational risk of the DPC's failure to uphold EU data rights*. https://www.iccl.ie/digital-data/ economic-reputational-risk-of-the-dpcs-failure-to-uphold-eu-data-rights

Ke, T. T. and Sudhir, K. (2020) Privacy rights and data security: GDPR and personal data markets. *Management Science* 69(8): 4389–412.

Kim, N. S. and Telman, D. A. (2015) Internet giants as quasi-governmental actors and the limits of contractual consent. *Missouri Law Review* 80(3).

Kusche, I. (2024). Possible harms of artificial intelligence and the EU AI Act: Fundamental rights and risk. *Journal of Risk Research*, 1–14. https://doi.org/10.1080/13669877.2024.2350720.
Luhmann, N. (2005). *Risk: A sociological theory* (1st paperback ed.). New Brunswick, N.J: Aldine Transaction.

Maggiolino, M.T. (2024) L'abuso di dipendenza economica nel mondo digitale. In S. Sileoni and C. Stagnaro (eds.), *Le sfide delle politiche digitali in Europa*, Turin (Italy): IBL Libri, 75-104.

Marques, N. and Portuese, A. (2023) Télécoms et innovation, donner la priorité à la création de richesse plutôt qu'à la redistributionTelecoms and innovation: How regulation is holding back 5G. Paris: Institut économique Molinari.

Maya-Salomé, G. (2023) The rule of law at risk: The dark side of the Digital Markets Act. *ORDO* 72-73(1).

Mayer, M. and Lu, Y-C. (2023) *Digital Autonomy? Measuring the Global Digital Dependence Structure*. Available at SSRN: https://ssrn.com/abstract=4404826 or http://dx.doi.org/10.2139/ssrn.4404826

Mchangama, J. and Callesen, L. (2022) *The wild west? Illegal comments on Facebook*. Copenhagen: Justitia.

Mchangama, J. and Alkiviadou, N. (2020) *The digital Berlin Wall: How Germany (accidentally) created a prototype for global online censorship - Act two*. Copenhagen: Justitia.

Mchangama, J. and Fiss, J. (2019) *The digital Berlin Wall: How Germany (accidentally) created a prototype for global online censorship*. Copenhagen: Justitia.

Mchangama, J., Alkiviadou, N., and Mendiratta, R. (2022) *Thoughts on the DSA: Challenges, ideas and the way forward through international human rights law*. Copenhagen: Justitia.

Monti, G. (2021) The Digital Markets Act – Institutional design and suggestions for improvement. TILEC Discussion Paper, DP 2021-004. Tilburg: Tilburg University.

Organisation for Economic Co-operation and Development (OECD). (2024). *Main Science and Technology Indicators: Business enterprise R&D expenditure as a percentage of GDP*. https://data-explorer.oecd.org.

Peukert, C., Bechtold, S., Batikas, M., and Kretschmer, T. (2022) Regulatory spillovers and data governance: Evidence from the GDPR. *Marketing Science* 41(4): 746–68.

Politou, E., Alepis, E., and Patsakis, C. (2018) Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity* 4(1).

Rességuier, A., & Rodrigues, R. (2020). AI ethics should not remain toothless! A call to bring back the teeth of ethics. *Big Data & Society, 7*(2), 1–12. https://doi.org/10.1177/2053951720942541.

Schiølin, K. (2020). Revolutionary dreams: Future essentialism and the sociotechnical imaginary of the fourth industrial revolution in Denmark. *Social Studies of Science, 50*(4), 542–566. https://doi.org/10.1177/0306312719867768.

Smuha, N. A. (2021) From a 'race to AI' to a 'race to AI regulation': Regulatory competition for artificial intelligence. *Law, Innovation and Technology* 13(1): 57–84.

Šonková, M. (2024) Brussels Effect Reloaded? The European Union's Digital Services Act and the Artificial Intelligence Act. College of Europe *EU Diplomacy Paper* 4/2024

Stagnaro, C. and A. Turillazzi (2022) Nothing lasts forever (even the gatekeeper's market share). Istituto Bruno Leoni *Special Report*, 12 April 2022.

Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU Artificial Intelligence Act. *Computer Law & Security Review, 43*, 105531. https://doi.org/10.1016/j.clsr.2021.105531.

Veale, M., Matus, K., & Gorwa, R. (2023). AI and global governance: Modalities, rationales, tensions. *Annual Review of Law and Social Science, 19*(1), 255–275. https://doi.org/10.31235/osf.io/ubxgk.

Veil, W. (2018) The GDPR: The emperor's new clothes - On the structural shortcomings of both the old and the new data protection law. *Neue Zeitschrift für Verwaltungsrecht* 10/2018:686–96.

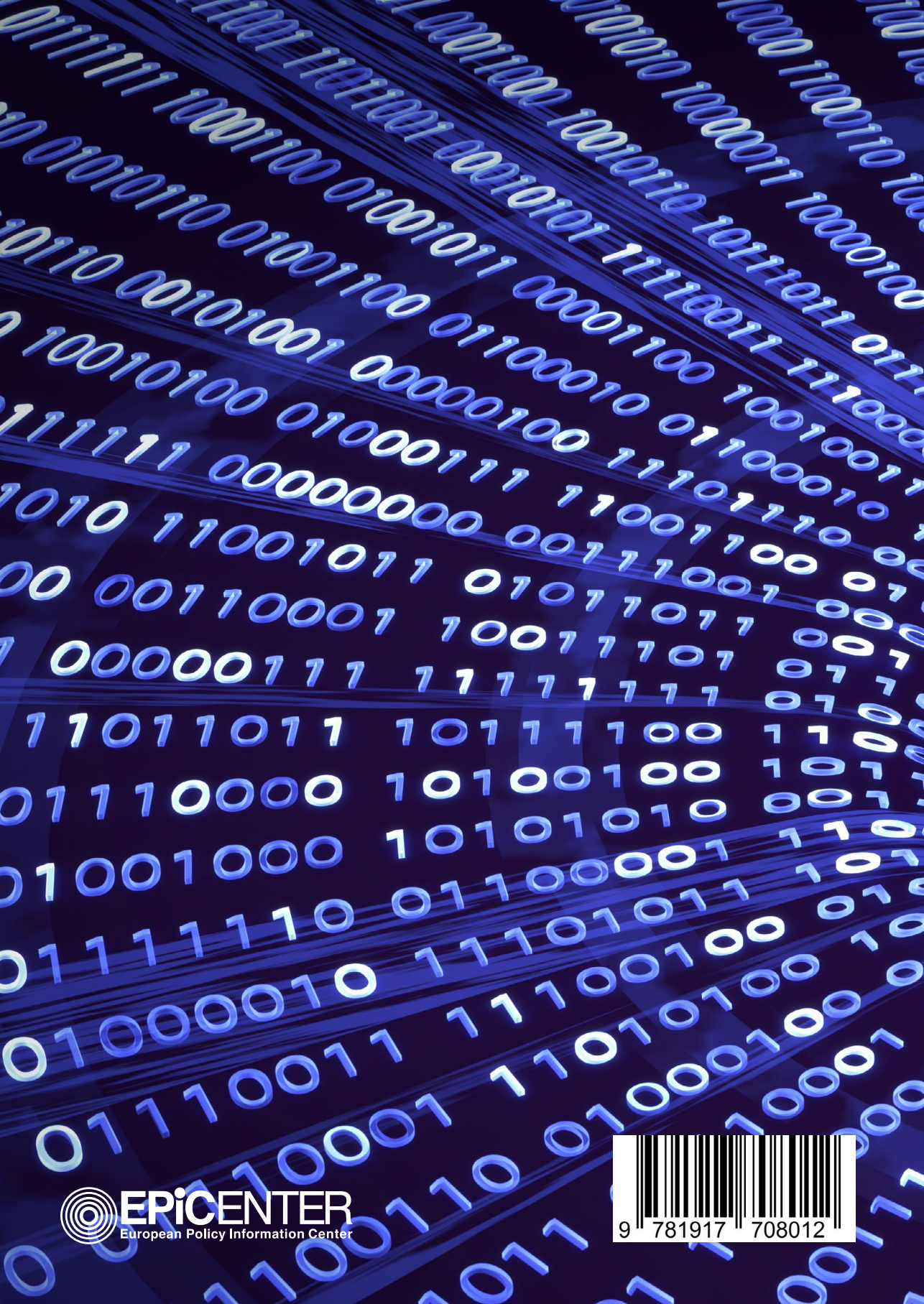
Von der Leyen, U. (2019) *Political guidelines for the next European Commission (2019-2024)*. Brussels: European Commission.

Wachter, S., Mittelstadt, B., and Russell, C. (2018) Counterfactual explanations without opening the black box: Automated decisions and the GDPR. *Harvard Journal of Law & Technology* 31(2): 842–87.

Wilman, F. (2022) The Digital Services Act (DSA) - An overview (https://ssrn.com/abstract=4304586).

Wörsdörfer, M. (2023) The Digital Markets Act and E.U. competition policy: A critical ordoliberal evaluation. *Philosophy of Management* 22(1): 149–71.

Zurth, P. (2021) The German NetzDG as role model or cautionary tale? Implications for the debate on social media liability. *Fordham Intellectual Property Media & Entertainment Law Journal* 31(4): 1084.


EPiCENTER
European Policy Information Center
9 781917 708012