CHARTING THE DIGITAL AND TECHNOLOGICAL FUTURE OF EUROPE:

WHAT PRIORITIES FOR THE EUROPEAN COMMISSION IN 2024-2029?

Views from the
European University Institute

Edited by
Klaudia Majcher

Report
December 2024

www.eui.eu

Co-funded by
the European Unior

Edited by

Klaudia Majcher
Research Fellow, Global Governance Programme, Robert Schuman Centre for Advanced Studies, European University Institute

Contributions by

Thorsten Beck
Full-time Professor and Director, Florence School of Banking and Finance, Robert Schuman Centre for Advanced Studies, European University Institute

Özlem Bedre-Defolie
Full-time Professor and Joint Chair, Department of Economics and Robert Schuman Centre for Advanced Studies, European University Institute

Lucía Bosoer
Project Associate, Florence School of Transnational Governance, European University Institute

Marco Botta
Part-time Professor and Scientific Coordinator, Centre for a Digital Society, Robert Schuman Centre for Advanced Studies, European University Institute

Elda Brogi
Part-time Professor and Deputy Director, Centre for Media Pluralism and Freedom, Robert Schuman Centre for Advanced Studies, European University Institute

Giacomo Calzolari
Full-time Professor and Dean of Research, Department of Economics, European University Institute

Marta Cantero Gamito
Research Fellow, Florence School of Transnational Governance, European University Institute

Roberta Carlini
Part-time Assistant Professor, Centre for Media Pluralism and Freedom and Centre for a Digital Society, Robert Schuman Centre for Advanced Studies, European University Institute

Danielle da Costa Leite Borges
Research Associate, Centre for Media Pluralism and Media Freedom and Centre for a Digital Society, Robert Schuman Centre for Advanced Studies, European University Institute

Primavera De Filippi
Visiting Fellow, Robert Schuman Centre for Advanced Studies, European University Institute

Niccolò Galli
Research Associate, Centre for a Digital Society, Robert Schuman Centre for Advanced Studies, European University Institute

Daniel Innerarity
Part-time Professor and Chair in AI & Democracy, Florence School of Transnational Governance, European University Institute

Morshed Mannan
Visiting Fellow, Robert Schuman Centre for Advanced Studies, European University Institute

Natalia Menéndez González
Research Associate, Centre for a Digital Society, Robert Schuman Centre for Advanced Studies, European University Institute

Iva Nenadić
Research Fellow and Scientific Coordinator, Centre for Media Pluralism and Freedom, Robert Schuman Centre for Advanced Studies, European University Institute

Pier Luigi Parcu
Part-time Professor and Director, Centre for Media Pluralism and Media Freedom and Centre for a Digital Society, Robert Schuman Centre for Advanced Studies, European University Institute

Patryk Pawlak
Part-time Professor and Project Director for the Global Initiative on the Future of the Internet, Robert Schuman Centre for Advanced Studies, European University Institute

Nicolas Petit
Full-time Professor, Head of Department and Director of Research, Department of Law, European University Institute

Anna Renata Pisarkiewicz
Research Fellow, Centre for a Digital Society, Robert Schuman Centre for Advanced Studies, European University Institute

Maria Alessandra Rossi
Part-time Professor, Centre for a Digital Society, Robert Schuman Centre for Advanced Studies, European University Institute

Giovanni Sartor
Part-time Professor, Department of Law, European University Institute

Thomas Streinz
Part-time Professor, Department of Law, European University Institute

Table of Contents

Preface

Klaudia Majcher, Giacomo Calzolari, Pier Luigi Parcu,
Nicolas Petit, Giovanni Sartor

This June, Europeans elected their representatives at the European Parliament. A new policy cycle is now starting. The appointment of a new European Commission marks more than just a change in leadership. It gives an opportunity to reflect on past achievements and to chart the course of the future of Europe.

Digital policies play a key role in shaping Europe's economy and society. Much is at stake: individual freedom, human rights, democracy, economic prosperity, social welfare, and the geopolitical position of Europe on the global stage. In recent years, Europe has strived towards achieving a just and human-centric digital transformation, introducing significant and innovative legislations. But Europe can do more to create more wealth and foster fairer, more sustainable, and inclusive social, economic, and political conditions.

This Report contributes to the conversation on the digital future of Europe. In an interdisciplinary spirit, it brings together researchers from distinct scholarly fields and methods –

professors, fellows and associates – working at the European University Institute (EUI) on the digital transformation. Each contribution is a short 'think piece' that translates academic ideas into policy recommendations. We chose a concise format in order to communicate clear messages to the policy arena. This Report offers a discussion framework, not ready-made solutions. The issues are complex, and definitive answers are far from reach. Our approach is to lay the groundwork for a forward-looking research agenda at the EUI and beyond. We hope to harness impactful scholarship and underline practical directions for addressing pressing policy challenges.

As a leading research university, the EUI provides a space for discussion, analysis, and engagement of all relevant stakeholders for the European common good: scholars, legislators, policymakers, and citizens. This Report illustrates the depth, breadth, and potential of such a reflection space in the digital sphere.

In this Report, we reflect on:

» How to foster competitive and innovative AI markets while ensuring that AI applications are safe and aligned with individual rights and social values?

» What interventions would be most effective in promoting fairness and consumer interests in markets in which large online platforms wield significant influence?

» What an innovation-friendly merger regime should look like?

» How to ensure consistency across the expanding array of digital legislation, including the Digital Markets Act, the Digital Services Act, the AI Act, the Data Governance Act and the Data Act?

» Which policies are vital to preserve an independent and pluralistic media ecosystem that serves democratic values?

» What policy and governance approaches merit prioritisation in light of technological advances like virtual reality and blockchain?

» And how can Europe effectively navigate its digital policy in an increasingly complex geopolitical global landscape?

This is not a complete list. This Report also touches on other pressing issues, reflecting the diversity and depth of scholarship undertaken at the EUI. That combination of expertise is vitally important. The boundaries between political power, corporate influence, market dynamics, individual rights, social values, emerging technologies, and geopolitical competition are blurred. Designing good digital policies in a complex world requires accommodating, challenging, and discussing diverse views and perspectives. A collaborative approach grounded in thoughtful and inclusive dialogue is essential. This Report can be viewed as a starting point, demonstrating the potential for engagement and interaction with lawmakers, policymakers, and society. We trust that the policy insights presented in this Report will make a valuable contribution to this important conversation about the future of Europe, in line with the appropriate role of a university in political and social action.

Florence

December 2024

01

A Global Perspective

Reconsidering the global dimension in regulating innovation

Pier Luigi Parcu and Maria Alessandra Rossi

The recent effort by the EU to regulate digital innovations seems to oscillate between the idea that it will be easy to impose its view globally (the 'Brussels effect') and caution to not hinder the innovation capacity of EU industries (the 'Draghi effect'). We suggest it is time to pause legislating on digital: the EU should concentrate on enforcing existing rules and on correcting their negative outcomes. In any case, adopting a balanced view on our position in the global dimension is the key to future action.

Challenges ahead

During the mandate of the last European Commission, the need to address several important concerns about the functioning of digital markets was tackled head-on by introducing a significant stack of new (and innovative) regulations, including the Digital Markets Act (DMA), the Digital Services Act (DSA), the AI Act, the Data Act and the Standard Essential Patent Regulation. All these regulations are driven by a dual rationale: to protect consumers while simultaneously creating opportunities for fair competition and innovation by EU firms.

While the aims of this regulatory effort are commendable, the sheer size of the recent EU *acquis* in the digital sphere may become a challenge for EU businesses. The idea that

the EU's leading position as a regulator in the global arena, the 'Brussels effect,' could constitute an advantage for European industry is perceived as less and less convincing. On the contrary, the possibility that a 'Draghi effect' predominates, i.e. that EU digital regulations end up being a drag on the productive and innovative efforts of EU firms, as has been recently suggested in the Draghi Report, is all too real. Quickly escaping this conundrum is a true challenge.

A second challenge concerns consistency. The complex and comprehensive regulatory effort undertaken in a relatively short timespan leaves space for possible contradictions and uncertainties on whether the various regulations will coherently converge. In particular, it should not be taken for granted that all the digital regulations will seamlessly integrate and contribute to the same vision of the role of Europe in the global economy. This suggests that a second major challenge will be to define a coherent vision of the geopolitical and geoeconomic role of Europe and ensure that digital regulations well serve the purpose of building up and strengthening this vision.

Policy priorities

In our view three policy priorities stand out as key in the next European Commission mandate. The first is to overcome the present inconsistencies in the conceptualisation of the role Europe should play in the geopolitical and geoeconomic arena and to define a coherent vision. The current emphasis on the need for Europe to leapfrog other countries in a range of technological races is often at odds with the role Europe has traditionally played in open and cooperative innovation, and particularly in the open internet. In addition, the a-critical reliance on the Brussels effect, in other words the notion that Europe may exert a global influence by virtue of its superior regulatory capabilities, risks being at odds with geopolitical realities and ultimately with the interests of EU firms and consumers. A political decision needs to be made on what overall vision should inform digital regulations.

The second policy priority is to take seriously the compliance and adaptation costs that EU firms face as a consequence of the newly introduced digital regulations. For some, like the DMA and DSA, there is an implicit understanding that their burden will be mostly on large foreign firms. But EU firms acting as suppliers and customers of these firms will inevitably be affected as well. Other regulations, like the AI Act, the Data Act and the Standard Essential Patent Regulation, impose direct costs on EU firms and constrain (often rightly) certain of their innovation activities. In both cases, it is imperative to pause the production of additional regulations for the duration of this mandate and concentrate

regulatory resources on designing appropriate forms of implementation. New regulations should only be introduced when they are perceived to be necessary to remedy the negative effects of existing regulations, and rigorous application of the one-in-one-out principle for adopting them should be strictly respected.

The third policy priority has to do with how digital regulation should prospectively evolve after the advocated pause. The time span of a Commission mandate is long enough to warrant caution in identifying specific themes to address after the necessary regulatory moratorium. Therefore, it is sensible to focus attention on the evolution of the methodology of regulation. From this perspective, a major 'missing link' in the design of current digital regulations is systematic acknowledgment of the fact that any desired impact of regulation on innovation by EU firms is strongly mediated by a geopolitical/geoeconomic dimension. This is something that features prominently in the debate on industrial policies and is practically absent from the regulatory landscape, mostly because of a tendency towards a-critical reliance on the Brussels effect. The impacts of regulation should be evaluated by taking into account the possibility that the Brussels effect does not materialise and by systematically considering all the pertinent feedback from the global economy.

For instance, in the case of the AI Act, the impact of this regulation could be re-assessed by considering the consequences for EU firms of the (likely) circumstance that the EU precautionary standard does not become a global standard, which has implications for the size of global demand EU firms will face. Therefore, the next mandate could be used to develop a framework to systematically analyse the geopolitical/geoeconomic effects and regulatory constraints and devise methods to introduce these evaluations in ex-ante impact assessments and in the periodic review. In the meantime, it is also opportune to re-examine from a geopolitical angle the most important digital regulations recently introduced and reconsider the specific effect on innovation by EU firms.

Stacking up for sovereignty: Charting Europe's digital future in a vertical world

Anna Renata Pisarkiewicz

As Europe faces critical technological challenges, the EU must adopt a holistic 'vertical stack' approach to digital sovereignty. This strategy should address interdependencies across the digital infrastructure, balancing innovation with strategic autonomy and ostering key partnerships to secure Europe's technological future.

Challenges Ahead

As the European Union stands on the cusp of a new technological era, the newly elected European Commission faces the critical task of shaping the digital and technological trajectory of the EU in an increasingly complex geopolitical landscape. The period from 2024 to 2029 will be critical for determining the position of Europe in the global tech arena, with far-reaching implications for its economic competitiveness, strategic autonomy, geopolitical influence and, last but not least, its democracy.

In recent years, technology has more than ever emerged as a central battleground in geopolitical struggles, with the concept of technological sovereignty gaining prominence. While this concept is still in need of defining principles, it reflects the ambition of the EU to strengthen or expand its technological leadership in areas where it is completely absent and to reduce dependence on foreign providers. However, the pursuit of sovereignty must be carefully balanced with the realities of the global and hyper-interconnected economy, global value chains and the need for strategic and symbiotic partnerships.

The EU's approach to technological sovereignty, including to the foundation of the digital economy, the internet, is distinct from that of the United States and China (Bradford, 2023), thus emphasising its value-based regulation and human-centric technology governance. This stance presents both challenges and opportunities as the EU seeks to navigate its relationship with global tech and political powers while asserting its own digital identity.

Discourse on the digital economy and technological sovereignty is currently undergoing a significant transformation. Historically, policymakers and industry experts approached related issues through a horizontal lens, focusing on individual sectors such as telecom infrastructure, cloud computing, big tech and semiconductors in isolation. This compartmentalised view reflected the early understanding of digital markets and the digital economy in which competition and innovation were primarily analysed focusing on specific markets, products or services.

However, as the digital landscape has evolved, so too has our understanding of its intrinsically interconnected nature. The emergence of platform ecosystems, in which tech giants create interconnected networks of products and services, has highlighted the limitations of this horizontal approach. Just as today we understand that digital platforms compete not just with individual products but on the strength and attractiveness of their entire ecosystems, we have come to understand that technological sovereignty and digital autonomy must also be approached holistically.

This shift in perspective has given rise to the concept of the 'vertical stack' in discussions on digital sovereignty and autonomy. Drawing on the ecosystem model of digital competition, the vertical stack acknowledges the interdependencies between different layers of digital infrastructure. While the vertical stack can be formulated in myriad ways, depending on the desired level of granularity, according to Sheikh (2022), for example, it consists of seven interconnected layers: resources, chips, networks, clouds, intelligence, applications and connected devices.

Geopolitical tensions ripple through the entire digital stack, affecting each layer in unique ways. Telecom networks act as the vital conduits of the digital economy, while semiconductors, for example, serve as the fundamental building blocks of digital technologies. By viewing these features as parts of an integrated system rather than isolated elements, we gain a more nuanced understanding of the challenges and opportunities involved in achieving technological sovereignty.

The EU telecom sector faces significant challenges, including declining average revenue per user (ARPU), insufficient investment and reliance on non-EU network equipment in critical infrastructure like 5G networks. The challenge for the European Commission will be to create an environment conducive to strengthening European telecom capabilities and promoting digital infrastructure in line with the Digital Compass 2030 goals while enhancing network security and addressing the 'fair share' debate between telecom operators and large tech companies.

The semiconductor industry is another critical area where geopolitical tensions intersect with technological sovereignty. The high dependence of the EU on external suppliers, in particular for the most advanced semiconductors, poses significant risks to its economic security and strategic autonomy. While the European Commission already adopted the Chips Act in 2023 to boost domestic semiconductor production in order to diversify its supply chain and reduce external dependencies, various commentators argue that its approach is misguided and wrongly focused and that rather than providing a meaningful long-term strategy the Act is but a collection of ideas and initiatives.

The recent Draghi Report (2024) commissioned by the European Commission addresses many of these challenges facing the digital and technological future of the EU. It highlights the need for a more unified approach to the telecoms sector and recognises the limitations of the EU in certain areas, such as advanced semiconductor manufacturing. It recommends focusing on strengthening areas in the value chain in which Europe is already present and emphasises the importance of boosting innovation, reforming industrial and trade policies, and increasing investment to close the gap with global competitors. While the report does not explicitly use the term 'vertical stack,' several of its recommendations align with the vertical stack approach and underscore the complexity of achieving technological sovereignty and digital autonomy across multiple interconnected layers.

Policy Priorities

Building an independent 'Eurostack' will require European Commission policy responses aimed at addressing existing dependencies in all seven layers of the vertical stack. This entails a re-evaluation of existing approaches to investment, regulation and the interaction among competition, regulatory and industrial policies. In the process of remaking policies, it will be particularly important to explore potential synergies in policymaking and approach different layers in a less horizontal and more holistic manner.

The concept of technological sovereignty, while crucial, requires clearer definition if it is to meaningfully shape EU digital policies. The key challenge for the Commission is to strike a balance between maintaining open, innovative, dynamic and diversified ecosystems while avoiding one-sided dependencies. Recognising this need, European institutions have already taken various steps to address the issue. For example, the European Parliament has produced a study on Key enabling technologies for Europe's technological sovereignty (2021) and the European Commission has proposed the Strategic Technologies for Europe Platform (STEP) initiative to support European leadership in critical technologies. To ensure complementarity of the efforts of its institutions, it is important for EU future initiatives to adopt coherent language and approaches to clearly define critical technologies, assess EU capabilities in different layers of the technological stack and develop strategies to secure the presence of the EU in the key parts of supply chains while fostering strategic international partnerships.

Therefore, as the European Commission charts the digital and technological future of the EU for 2024-2029, it must navigate a complex landscape of geopolitical tensions, technological dependencies and economic challenges. Only by focusing on key sectors like telecommunications, semiconductors, clouds, AI etc. while examining synergies between them will the EU have a chance to address the broader issue of technological sovereignty. The success of these efforts will depend on its ability to leverage its strengths, including its large internal market, strong research base and commitment to ethical technology development, while fostering strategic partnerships and addressing its main shortcomings, namely the lack of access to sufficient capital.

Advancing digilateral foreign policy

Patryk Pawlak

The EU must abandon its piecemeal approach to governing digital, cyber, tech and information spaces and develop a digilateral foreign policy doctrine implemented through a dedicated inter-institutional task force and a comprehensive accountability toolbox.

Challenges ahead

The main focus of the next European Union leadership will be on ensuring that the period of intensive regulation and policy entrepreneurship during the first von der Leyen's Commission is followed by proper monitoring and implementation. The mission letter of Henna Virkkunen – the incoming Executive Vice-President for Tech Sovereignty, Security and Democracy – clearly articulates the need to host implementation dialogues with stakeholders to align implementation with realities on the ground and prepare an Annual Progress Report on Enforcement and Implementation for parliamentary committees and council bodies. These are welcome developments that will strengthen the transparency and accountability of the College of Commissioners and the member states.

However, changing the guard in Brussels is occurring at a time when the protection of human rights online has been in decline globally for the fourteenth consecutive year. This means another increase in the number of countries implementing policies legitimising censorship, content manipulation, limiting freedom of expression and interference in electoral processes. At the same time, the scale and complexity of malicious cyber operations and foreign information manipulation and interference (FIMI) against the EU, its member states and allies has also increased, posing a threat to the proper functio-

ning of democratic institutions and processes, business operations and citizen well-being.

This interference directly challenges the EU vision of human-centred digital transformation built on open free, secure, and global cyberspace, in which the rule of law and human rights are adequately protected. Therefore, this contribution argues that a key priority for the new leadership should be to strengthen, protect and promote the EU vision of governance of the digital, cyber and information spaces in an increasingly contested world. The lack of a joined-up approach to addressing the governance challenges posed by this complex ecosystem has undermined the EU's capacity to act and goes against the general trend among its partners. Australia's 2023-2030 Cyber Security Strategy addresses cyber and critical technology as foreign policy priorities. The Bureau of Cyberspace and Digital Policy (CDP) at the U.S. Department of State has been reorganised to promote national and economic security by leading, coordinating and elevating foreign policy on cyberspace and digital technologies. In the EU, on the other hand, cyber and digital issues, hybrid threats and foreign interference are being dealt with separately and by different parts of the European External Action Service. In addition, the important role played by the European Commission as the owner of significant resources for these policies – including their international dimension – has

made a coherent international cyber policy more complicated.

Policy priorities

EU foreign policy needs a new vision that reflects the central roles of digital, cyber, tech and information spaces in achieving the priorities of the Union and protecting its interests in the increasingly polarised international environment. Together, they create an interdependent ecosystem encompassing the full scope of virtual, technological and information environments that are critical in the conduct of EU foreign and security policy. This link with foreign policy was well-captured by previous High Representative Josep Borrell: "We, Europeans, we have been norm setters because we have been technological leaders. If we lose the leadership of technologies, we will not be able to continue being the norm setters." Therefore, decisions about technological governance will ultimately strengthen or limit the influence and ability to act of the EU.

First, the EU should adopt digilateralism as a doctrine in its foreign and security policy. This doctrine explicitly recognises the importance of interlinkages between the digital ecosystem and EU relations with partner countries at the bilateral, regional and multilateral levels. As digital transformation and new technologies are at the foundations of

our societies, the rights and obligations that result from the governance choices made by individual states will decide on our collective digital future. Digilateralism is a bridge between the EU's different approaches to governance in all areas. Its primary focus is on acknowledging that digital, tech, cyber and information spaces are critical to the EU's interests and therefore the EU needs to make decisions about governance a central piece of its foreign policy engagement. This is what China and Russia understood and put into practice decades ago. The EU's standards, norms and principles need to become a part of its diplomatic agenda. At the same time, the EU regulatory frameworks should be used to make global non-binding and voluntary norms binding – within the EU and globally through extraterritorial application. Such approach would ultimately contribute to strengthening the rules-based global order. Whether on data protection, AI or green tech, the EU has the instruments to ensure broader compliance. Establishing a dedicated interinstitutional task force led by High Representative and Vice-President Kallas and Vice-President Virkkunen – similar to the Security Union Task Force established in the past by Commissioner Julian King – could be the first step.

Second, the EU should work towards a comprehensive accountability toolbox for the digital ecosystem that will end impunity of malicious actors and those violating human rights online. In recent years the EU has developed and put in place several toolboxes that address different spaces: a Cyber Diplomacy Toolbox to prevent, discourage, deter and respond to malicious cyber activities; a Hybrid Toolbox to detect and build resilience against hybrid operations; and an FIMI Toolbox comprising measures and structures to systematically detect and expose FIMI. This artificial separation of foreign policy instruments is unsustainable as it reinforces silos mentality and leads to duplications, which in the long term put pressure on already scarce resources. All these toolboxes share the same main purpose, which is to end the impunity of the perpetrators and make malicious actors accountable for their actions. Therefore, merging all existing mechanisms into a single comprehensive accountability toolbox (CAT) would make the existing tools mutually reinforcing, allowing a joined-up response. The adoption in October 2024 of a new framework for restrictive measures in response to Russia's destabilising actions abroad is a step in the right direction. It will allow the EU to comprehensively address complex threats such as undermining electoral processes and the functioning of democratic institutions, sabotaging critical infrastructure, using coordinated disinformation and malicious cyber activities.

Developing a truly digilateral foreign policy with a robust comprehensive accountability toolbox will require reviewing the working methods and institutional structures as well as entail a significant investment in human capital. The alternative is the business as usual where the EU continues to punch below its weight.

02
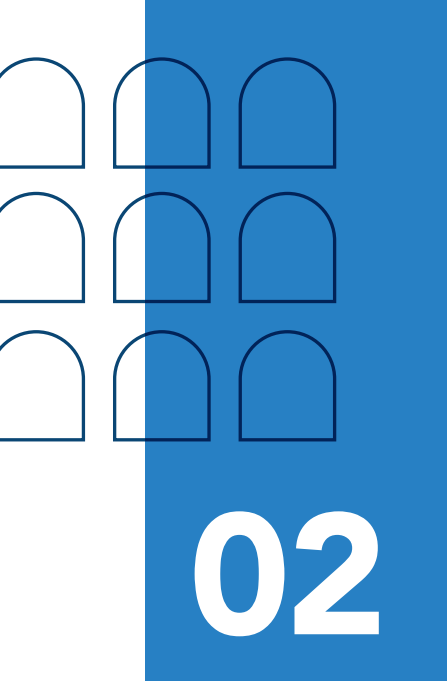
Competition and Innovation

Promoting competitive and innovative AI markets

Giacomo Calzolari

AI has vast potential to drive innovation and growth and enhance public welfare. However, policymakers must be prepared to act more swiftly than in the past to ensure timely intervention to prevent market concentration and ensure that the benefits of AI are broadly shared in a competitive, inclusive and novel ecosystem.

Challenges ahead

AI is poised to spark a revolution in economies and markets. It is one of the most transformative technologies in the modern era and it presents unprecedented opportunities to reshape industries, improve public welfare and address critical societal challenges like climate change, healthcare and infrastructure. However, its transformative power also brings significant competition concerns. What sets this moment apart is the unprecedented context in which it unfolds. We are entering this AI revolution while the adjacent digital market is already highly concentrated, and Europe has very few relevant companies competing in these critical sectors. Dominant firms in digital platforms control vast resources such as data, computing infrastructure, and user networks, which they can leverage to gain an advantage in the rapidly growing AI market.

The AI industry itself has characteristics that may naturally lead to market concentration. Large datasets, access to advanced computing power and specialised talent are all critical inputs for developing cutting-edge AI models, and firms that can consolidate these resources can gain and exploit significant market advantages. However, despite these tendencies, we have not yet seen a very concentrated AI market. Healthy competition still exists in key areas of AI development, with smaller firms and open-source projects contributing to innovation.

AI applications further complicate the competitive landscape. AI-driven systems like pricing algorithms, recommendation engines and autonomous solutions can distort competition, leading to outcomes such as algorithmic collusion, price manipulation and biased content delivery. AI's ability to exploit data and behavioural insights risks further entrenching the dominance of large platforms and restricting new entrants.

Recent advances in generative AI represent both a significant leap forward in AI capabilities and a potential shift in the competitive landscape. Generative AI, with its ability to create text, images and even software, introduces new challenges for competition policy. These technologies often depend on vast datasets and advanced infrastructure, which may further consolidate the market position of tech giants with access to such resources. In this context, the European Commission must closely monitor the emerging market evolution of generative AI developments to ensure that smaller companies and open-source initiatives remain competitive players. This area represents a critical frontier in which current regulations may need to be adapted or expanded.

These risks in the AI market and its applications are significant and far-reaching, to some extent preceding those addressed in the European AI Act. The critical challenge for policymakers is to act swiftly while striking the right balance – to ensure a level playing field, foster healthy competition and enable AI to reach its transformative potential across sectors – and thus enhance the long-term competitiveness of Europe.

Policy priorities

To fully harness the transformative potential of AI, swift and proactive action is required to ensure competition remains healthy in both the AI market and its applications. Bold policies may soon be necessary to keep AI markets competitive and avoid the concentration pitfalls seen in previous technological revolutions.

In the AI market, it is essential to prevent the dominance of a few firms over key resources like data and cloud infrastructure. Antitrust measures must ensure that access to these resources remains fair and open, and merger and acquisition reviews should be expanded to include not only full acquisitions but also strategic partnerships and minority stakes that could lead to anti-competitive outcomes. In fact, the landscape of M&A in the AI sector has evolved, bringing to light new practices like 'acqui-hires,' in which companies are acquired primarily for their talent rather than their technology or market share. This trend raises concerns that need to be addressed in antitrust frameworks. To respond effectively, the Commission should consider extending the scope of M&A reviews to capture tradi-

tional mergers and these talent-driven acquisitions alongside partnerships and minority stakes.

Data-sharing mandates and rules ensuring non-discriminatory access to cloud computing services and AI infrastructure will help prevent monopolisation and support innovation, allowing smaller firms and start-ups to compete.

Industrial policy should complement these efforts by fostering investment in AI infrastructure. Governments must promote collaborative innovation and public-private partnerships that enable broad participation in AI development to ensure the market remains dynamic and diverse.

For AI market applications, regulations must ensure transparency, fairness, and competition. Algorithmic transparency and auditing are critical to prevent algorithmic collusion, price discrimination and anti-competitive practices in sectors such as e-commerce, finance and telecommunications. AI-powered systems must adhere to standards that protect consumers and foster competition and prevent large platforms from using AI to manipulate consumer behaviour or exclude competitors. In industries such as healthcare, finance and transport, ensuring open access to AI-driven data and tools will be vital to maintain innovation and prevent dominant firms from monopolising entire industries.

Ethical AI standards and privacy-enhancing technologies should be prioritised to safeguard consumer data and trust while promoting competitive and innovative AI markets. By acting more swiftly and with a forward-looking approach compared to the past, and with a combination of strong regulation and robust industrial support, Europe can ensure that the benefits of AI are widely shared, thus advancing both innovation and public welfare.

While existing regulations such as the Digital Markets Act, the General Data Protection Regulation and the AI Act are robust frameworks to address the challenges posed by the digital economy and AI, they may not be fully sufficient to cover the rapidly evolving AI market and its unique competitive dynamics. For instance, current antitrust rules, despite being comprehensive, may require additional tools or reforms to address new risks associated with the AI landscape. The Commission must focus on stringently enforcing these regulations to ensure a level playing field, but there may also be gaps that necessitate new rules. The rapid evolution of the AI sector, particularly regarding access to critical resources such as data and computing power, requires a more agile regulatory approach, which can include extending existing legislation and introducing novel provisions to regulate new issues.

Challenging assumptions in competition policy concerning large European firms, competition and innovation

Nicolas Petit

The competitiveness agenda calls for increased business consolidation and a more pro-European competition policy.

Challenges Ahead

Behind diplomatic language, the Draghi report conveys critical insights about competition. Unlike the US, the EU lacks 'dynamic competition' by technology enabled businesses which supply high surpluses to users and hence can sell their services at a higher price than other firms. Like the US, the EU lacks 'static competition,' as visible in rising concentration, price-cost margins and the size of businesses since the 1980s. In current discourse, the risk is that these findings will be distorted.

From this, some may be tempted to infer that more competition law enforcement is needed.

Any such interpretation is a non sequitur. Saying that economic competition is weak is one thing. Saying that more enforcement of competition law is necessary is another one. Draghi says the former, not the latter. In particular, Draghi's policy proposals clearly indicate that the current approach to enforcing competition law has not and does not bring about the gains expected in theoretical and empirical studies. Hence, the Draghi report suggests that competition policy "need to be adapted to the radically changing world." Draghi indicates three directions for a revamped competition policy: first, developing a competition policy that is more open to business consolidation; second, formulating a competition policy that is more

favourable to European firms; and third, enabling EU aid and disabling national aid. All three propositions are likely to be extremely controversial.

Policy Priorities

M&A is the competition policy priority. The EU should revise its merger guidelines to introduce an effective 'innovation defence.' The defence should provide examples of innovation efficiencies, including 'fixed cost efficiencies.'

The merger guidelines – and perhaps the remedy notice – should integrate a 'contractual' framework to allow merging firms to benefit from a clearance decision in exchange for a verifiable efficiency or innovation investment plan. The European Commission (EC) should study examples in past consent decrees that credit efficiencies in exchange for behavioural modifications. For example, the US FTC approval of the joint venture between General Motors and Toyota in 1984 recognised efficiencies but subjected the transaction to strict restrictions in the following years.

The EC merger practice in specific sectors will need to engage with calls for it to adapt. The EC should broadly consult in order to avoid any extreme view. Some suggestions regarding facilitating consolidation of telecom markets

in the Draghi report will trigger polarisation. On the one hand, some observers will oppose any further concentration of telecom markets on the ground of risks of short-term price increases. On the other hand, some industry stakeholders will do anything to enforce the view that telecom suppliers must consolidate because they are the best positioned to leverage opportunities arising from digitalisation of the economy. A middle ground could be to chart a clearance course for telecom mergers involving pan-European integration not national consolidation.

A more ambitious reform of competition policy may also seek to enable the EC or another political institution to 'pick mergers' and accept those that it likes best from a European competitiveness or resilience standpoint. In all industries there is a finite set of possible M&A transactions. The EU institutions may have to ask themselves about alternative M&A combinations when reviewing transactions and defining an order of preference for future transactions. This would require adopting a clear substantive procedural framework anchored in hard facts to avoid the risk of excessive discretion.

One option would be to allow appeals against EC administrative decisions to a third-party body conditional on limitation of the grounds for appeal against a merger decision. In turn, the appeal body would be empowered to

overturn EC merger decisions on grounds of 'innovation potential,' either because a forbidden anticompetitive merger would give rise to increased innovation capability or because a cleared procompetitive merger would pre-empt better innovation capability configurations.

In any case, revising merger guidelines will require much technical work by competition policy experts. As was the case in prior episodes of modernisation of competition policy, time is ripe for a process of disciplined heterodoxy toward scientific fields the core subjects of which are dynamic competition, innovation capabilities and business and management science. That reform process will need to be grounded in facts, empirics and economics. This disqualifies a limited number of the proposals in the Draghi report, like the idea of defining markets more broadly by default.

Designing policy interventions to foster competition and innovation in digital markets

Özlem Bedre-Defolie

Digital marketplaces have become 'gatekeepers' for millions of consumers and third-party businesses trading. Their rising market power and business practices have raised significant concerns among antitrust and regulatory agencies around the world. Policymakers need to understand which interventions should be put in place to make digital markets more competitive so that consumers benefit from greater variety, better quality, lower prices and more innovation.

Challenges ahead

Digital marketplaces enable trade between consumers and third-party service/product providers (sellers), e.g. Amazon, Apple and Google Play app stores, which collect commission on revenue generated by sellers and fees for add-on services. Most run a 'hybrid business model:' they sell their own products (1st-party products and/or private labels) and host 3rd-party products.

Dominant hybrid platforms might distort competition in the marketplace due to their dual roles as both referees and players. Important policy concerns include whether the hybrid mode of dominant platforms harms 3rd-party sellers and consumers, whether they charge 3rd-party sellers too high commission and fees, and whether they impede entry and innovation by other platforms or sellers with contractual provisions. These concerns have been at the centre of recent important cases

in Europe (European Commission cases against Amazon, Google and Apple) and in the US (Epic Games lawsuits against Apple and Google, the Federal Trade Commission lawsuit against Amazon, the US Department of Justice lawsuits against Apple). Recently, the EU Digital Markets Act and the Digital Services Act have banned certain practices and imposed rules on gatekeeper platforms.

Effective and proportionate implementation of the DMA and DSA are important challenges ahead for EU policy makers. They need to clarify the obligations of gatekeepers and how compliance with these obligations is to be assessed and demonstrated. They also need to respect proportionality to avoid harming innovation and consumer choice. Economic analysis is essential to address implementation challenges and to assess which regulations/interventions are essential in order to make digital markets more competitive and foster innovation.

Policy priorities

Policymakers have argued that gatekeeper platforms could harm consumers and 3rd-party sellers with excessive fees for 3rd-party sellers, self-preferencing, using 3rd-party sales data in own product decisions, and restricting or punishing the use of alternative platforms, e.g. 3rd-party payment systems. The DMA bans these gatekeeper platform practices.

To achieve regulatory objectives while not harming innovation and consumer choices, it is essential for policymakers to clarify exactly which dominant digital platform business practices are banned, how these practices can be distinguished from legitimate competitive practices and what kind of evidence is needed to prove that these practices are not taking place. For example, the DMA prohibits 'self-preferencing.' It should clearly specify what kinds of practices are considered self-preferencing, to what extent fees associated with rankings (sponsored links) and fees for add-on services (like fulfilment) to guarantee higher placement or quality labels (like 'Prime') are subject to the ban, and how it can be proved that there is no bias when rankings are based on AI-based self-learning algorithms.

It is necessary to use careful economic analysis to identify whether banned practices occur in practice and to evaluate the effects of different regulatory measures in order to ensure that regulations are in line with their objectives. Understanding the incentives and business models of platforms and identifying the factors that affect these incentives and the choice of certain business models or contractual provisions are essential to predict the reactions of dominant platforms to regulatory provisions, and consequently to evaluate the effects of different regulatory measures. Policymakers should take a minimalist appro-

ach in terms of the depth and breadth of regulations to avoid unintended consequences, like digital platforms stopping offering certain valuable services or reducing their investments in innovations.

Digital markets are characterised by dynamic radical innovations, like AI-based innovations such as ChatGPT, which can drastically change competitive forces and make some regulations redundant and harmful. Policymakers should update their approaches and toolboxes to adjust to changing market conditions and new technologies. Their interventions should not limit incentives to innovate and compete for the market.

Acquisitions of startups in complementary markets could enable dominant platforms to expand their market power from one market to another, dampen future competition and generate 'ecosystems' within which dominant platforms could increase their market power via data spillovers and strategies tying their dominant segment to competitive ones. Policymakers should take a close look at such acquisitions to evaluate potential anti-competitive effects, ensure consumer benefits and foster incentives to innovate.

Effectively enforcing the Digital Markets Act

Marco Botta and Pier Luigi Parcu

To ensure effective enforcement of the Digital Markets Act, the European Commission should immediately identify indicators and benchmarks to assess its impact on fairness and contestability, engage in regulatory dialogue with gatekeepers, widely involve third parties in its investigations, intensify cooperation with National Competition Authorities and adopt a set of measures to allow scrutiny of concentrations by gatekeepers in the aftermath of the Illumina-Grail ruling.

Challenges ahead

Following the entry into force of the Digital Markets Act, the European Commission designated Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft and more recently Booking as digital gatekeepers, making them subject to DMA obligations. In March 2024, the first designated gatekeepers submitted their compliance reports. Generally unsatisfied with the reports, the Commission launched non-compliance investigations: Meta faces scrutiny over its 'pay or consent' model, while Google and Apple are accused of limiting the ability of app developers 'to steer' users outside GooglePlay and the App Store. In addition, Google faces proceedings on self-preferencing its own search services, while Apple is accused of limiting the installation of third-party apps and app stores on iOS. Finally, in September 2024 the Commission started two specification proceedings to assist Apple in complying with its interoperability obligations under the DMA.

Challenges ahead for the next Commission in terms of DMA enforcement include completing the market investigation into the designa-

tion of X (formerly Twitter) as gatekeeper by the end of 2024 and reviewing Booking's compliance report. The Commission must also complete the pending infringement investigations concerning Meta, Apple and Alphabet by March 2025, and finalise the specification proceedings with Apple.

To sum up, the Commission has started to actively enforce the DMA, but questions remain regarding its ability to advance the declared aims of fairness and contestability in today's digital world. Piecemeal interventions targeting the behaviour of individual companies may struggle to shape a coherent evolution of the European digital landscape.

Policy priorities

As the European Commission actively enforces the DMA, it should concentrate on a few key priorities to ensure the effectiveness of the regulation. The first concerns indicators and benchmarking. As Article 53 DMA stipulates, three years after the entry into force of the DMA (i.e. 3 May 2026) the Commission has to carry out an evaluation of the impact of DMA obligations on end and business users. A recent CERRE report argues that "the Commission should already today prepare the evaluation by determining which indicators should be collected, by whom, and how." A year after the first decisions on designating gatekeepers, the Commission should immediately start to define qualitative and quantitative indicators and benchmarks to assess whether and to what extent the DMA is increasing the fairness and contestability of various core platform services. Benchmarking would be important to forecast long-term trends in competitive dynamics in digital markets and could support the Commission in the ongoing infringement investigations.

Second, the Commission should ensure timely enforcement of DMA obligations. The Commission can close the pending infringement investigations into Apple, Meta and Alphabet either with infringement decisions or with commitments offered by the gatekeepers. On the one hand, by adopting infringement decisions, the Commission would show its teeth as a credible enforcer. On the other hand, the decisions are likely to be appealed, leading to lengthy judicial proceedings in the courts in Luxembourg. One of the reasons for adopting the DMA was the slowness of antitrust ex-post intervention. However, it is unclear how the DMA will facilitate speedier intervention, unless the Commission pushes for and obtains from the gatekeepers widespread acceptance of commitment decisions.

Furthermore, the Commission should engage more frequently in regulatory dialogue. Specification proceedings, such as those currently ongoing with Apple, could show a pathway for interaction between the Commission and gatekeepers. According

to Article 8(3) DMA, such dialogue may concern the obligations in Articles 6 and 7 DMA. Gatekeepers can request specification proceedings to be opened, but the Commission has the discretion to accept or decline these requests. The Commission can always revert to non-compliance proceedings if specification proceedings are unsuccessful. In the coming months, the Commission could engage in a regulatory dialogue with other gatekeepers beyond Apple. In particular, it could temporarily suspend the ongoing infringement investigations against Google and Apple for breaches of Article 6 DMA. This regulatory dialogue could be more effective than infringement proceedings in ensuring effective compliance with the DMA.

The Commission should also engage in cooperation with interested third parties during the infringement investigations, particularly given the complexity of DMA investigations, the limited technical resources and timeframe of the Commission, and its dependence on information provided by gatekeepers. The information asymmetry in the enforcement of digital regulations appears to be a major hurdle that needs a well-thought-out strategy. The Commission's public workshops since the entry into force of the DMA demonstrate its intention to involve third parties. The same approach should be adopted in the infringement investigations. Opinions from competitors of gatekeepers, business users and consumer associations may become essential for the

Commission to collect independent relevant evidence on DMA compliance.

Cooperation with national competition authorities (NCAs) should be another priority for the Commission. NCAs are actively involved in enforcing the DMA, thus supporting the Commission in collecting evidence and complaints. NCAs may also investigate and sanction infringements of the DMA if the national law grants them this power. A recent study shows that most NCAs are now empowered to do this. However, diverging decisions by NCAs might jeopardise the functioning of the internal market. One of the reasons for adopting the DMA was to prevent fragmentation of the EU single market due to varying regulatory interventions in member states. Unlike Regulation 1/2003, the DMA is not based on a decentralised system of enforcement. Therefore, the Commission should actively exchange information and monitor national investigations into DMA compliance. Using Article 38(7) DMA, the Commission should actively prevent decisions by NCAs by opening its own investigations into the same cases. Exchanging information and periodic meetings with NCAs, along with active reliance on Article 38(7) DMA, could prevent diverging regulatory outcomes that may restrict the free movement of digital services in the EU and so hamper the competitiveness of the European economy.

A final point concerns information about concentrations. According to Article 13(1) DMA, gatekeepers must inform the Commission of "any intended concentration" regardless of whether the transaction meets the turnover thresholds in the EU Merger Regulation (EUMR). At the same time, in line with 2021 Commission Guidance on Article 22 EUMR, the Commission can inform the EU member states about potentially problematic concentrations by gatekeepers allowing national authorities to request formal notifications by the merging parties. However, in the recent *Illumina/Grail* ruling the European Court of Justice found that the Commission's expansive interpretation of Article 22 exceeded its intended scope. The Court held that Article 22 EUMR does not apply to transactions that are not covered by either EU or national merger rules, underscoring that Article 22 EUMR was not designed as a 'catch-all' corrective mechanism. The *Illumina/Grail* judgment may significantly affect the information duty in Article 13 DMA. While this duty formally remains in place, it is *de facto* impossible for the Commission to rely on Article 22 to request formal notifications by the merging parties. As has recently been <u>recognised by Executive Vice-President Vestager</u>, this issue can only be addressed with a legislative amendment to the EUMR, such as lowering turnover thresholds, introducing value-ba-

sed thresholds and allowing the Commission to review below-threshold concentrations in specific situations. Unfortunately, such legislative amendments are likely to take a long time to materialise. The Commission should therefore consider alternative solutions to make the DMA Article 13 information procedure effective. First, in accordance with the <u>*Continental Can*</u> case law, the Commission could *ex-post* review below-threshold concentrations in accordance with Article 102 TFEU. In addition, the Commission could share information gathered according to Article 13 DMA with NCAs, allowing them to review below-threshold concentrations in accordance with Article 102 and in line with the <u>*Towercast*</u> case law. Finally, and more importantly, the Commission could engage in a regulatory dialogue with the gatekeepers, encouraging them to voluntarily notify potentially problematic concentrations to prevent ex-post scrutiny in accordance with Article 102 TFEU.

Reforming the framework for licensing standard essential patents

Niccolò Galli

In the shift from patent and antitrust principles to ex-ante regulation of Standard Essential Patent licensing, the European Commission and the EU Intellectual Property Office should maintain the balance between developers and implementers of ICT standards to preserve the standardisation ecosystem.

Challenges ahead

The EU intellectual property (IP) policy framework faces several challenges, both structural and dynamic, due to the complex European legal system and the societal transformation brought about by digitalisation respectively. The core challenge remains putting into practice the social contract between society and creators regarding the protection and use of intellectual property, which must balance the limited exclusive rights of creators with knowledge diffusion in the public interest. Among the contemporary IP challenges, such as the tension between pharmaceutical innovation and affordable access to medicines and the underutilisation of the IP system by resource-constrained stakeholders, the functioning of the information communication technology (ICT) standardisation ecosystem emerges as a particularly delicate policy area.

The digital economy relies on coordinated efforts by industry participants to establish ICT standards through standard-development organisations (SDOs) to better meet consumer demand for interoperabili-

ty, connectivity and innovation in a timely fashion. The diffusion of global standards such as 5G or Wi-Fi 7 drives economic growth and prosperity by enabling the internet of things (IoT) and the fourth industrial revolution. However, as ICT standards evolve into general-purpose technologies and transcend the boundaries of traditional computer and telecommunications industries, tensions arise regarding licensing the patents declared essential for their implementation (i.e. standard essential patents, SEPs). Under the fair, reasonable and non-discriminatory (FRAND) licensing commitments made to SDOs, SEP-holders seek remuneration from implementers, which in the IoT context are often newcomers to FRAND licensing. For example, manufacturers of new smart products, such as intelligent vehicles and connected meters, lack experience in implementing ICT standards and negotiating FRAND licenses. Implementers resist SEP licensing demands using the patent hold-up argument, namely that SEP holders request higher than FRAND compensation, often leveraging opportunistic patent litigation. SEP holders counter with the patent hold-out assertion, claiming that bad faith implementers strategically avoid taking out FRAND licenses and instead efficiently infringe SEPs. Such commercial disputes lead to patent litigation and antitrust complaints, with each side attempting to gain an advantage in the licensing negotiation. As a result, judges and antitrust officials face the quasi-regulatory task of fairly allocating standardisation benefits among the litigants – essentially putting a price tag on FRAND licenses. Both over-compensation and under-compensation of SEP holders risk undermining confidence in and incentives to join SDO open innovation efforts, tilting the balance towards less inclusive organisational forms which are subject to their own market failures. Think of the interoperability issues of proprietary standards set by vertically integrated firms, the wasteful duplication of investments for competing regional standards and the unfairness issues in gatekeeping platform ecosystems.

Policy priorities

Despite the global nature of ICT standardisation, prominent economies are dealing with SEP licensing and litigation mainly from a national or, at best, regional policy perspective, in line with the 'balkanisation' of industrial policies. In contrast to China, Japan, the UK and the US, which opted for non-regulatory or soft-law approaches to SEP licensing, in 2023 the Commission presented a SEP regulatory proposal. The proposal envisages changing the European legal framework for administering and licensing SEPs, which so far has been based on patent and competition laws. If enacted, it would impose registration of SEPs in an electronic register held by the

EU Intellectual Property Office (EUIPO) for the patentee to enforce its rights in the EU. Furthermore, the EUIPO would administer non-binding procedures to assess the essentiality of registered SEPs, establish global aggregate royalty rates for implementation of standards and determine actual FRAND licenses. However, the EU proposal still leaves several crucial issues open.

Above all, the regulatory scope is uncertain. In principle, the proposed regulation applies to standards published after it enters into force. However, the Commission would have delegated power to exclude new standards or use cases from certain aspects of the regulatory regime and include existing standards or use cases depending on their licensing efficiency or distortion respectively (see Arts. 1(4) and 66(4) of the Proposal). The Commission's priority should be to provide standardisation stakeholders with predictability and establish an objective and fact-based methodology that clarifies which licensing efficiencies or distortions determine the regulatory scope. This methodology should also be practical and self-executing without requiring labour-intensive regulatory monitoring of all the markets affected by standardisation.

Furthermore, given the uncertain impact of the new regulatory regime on standardisation, which might be hindered if SEP holders do not receive adequate remuneration for their standardisation investments or if imple-menters overpay for access to standards, the Commission should adopt a cautious approach to the regulatory scope. A lack of market adoption should lead to exclusion of new standards or use cases from the regulation while allowing the inclusion of older ones. Conversely, widespread market diffusion should justify keeping old standards and use cases outside the regulation and incorporating new ones in it. In this way, the Commission would ensure consistency of the regulatory regime with ongoing and future standardisation efforts.

Finally, the Commission should address the issue left out of the proposed regulation of where to license SEPs along the value chains of IoT verticals, whether at the component level (e.g. the chip or connection module) or end product level (e.g. connected vehicles or smart meters). Here, guidance should come from EU competition law, particularly from the revised block exemption regime for technology transfer agreements, which applies to SEP licenses, and from the enforcement practice that further specifies the abuse of the dominance negotiating framework established by the CJEU in _Huawei/ZTE_. In so doing, the Commission must ensure that both sides of the standardisation table remain incentivised to invest in developing and implementing standards in Europe, so that neither side loses out to non-EU markets.

03

Technology and Society

Implementing the AI Act

Giovanni Sartor

In implementing the AI Act, European and national regulators must proactively engage with developers, deployers and civil society in an effort to ensure that AI applications are safe and trustworthy, and respect individual rights and social values without affecting useful deployments of AI and the competitiveness of EU industry.

Challenges ahead

On 13 June 2024, the AI Act was approved, bringing to completion a legislative process that started with a 2021 Commission proposal and was preceded and accompanied by a large debate involving European and national institutions, legal, ethical and technology experts, and AI companies and civil society. The AI Act is a key element in the EU effort to regulate digital technologies and it complements other instruments such as the General Data Protection Regulation, the Digital Services Act, the Digital Markets Act and the Data Act. It shares with these instruments the aim to govern digital technologies with a uniform EU-level legal framework which provides substantive and procedural norms, and implementation mechanisms.

While AI has been around for many years, the need to regulate it has only emerged since the recent development of effective machine learning technologies. This has enabled AI to be successfully deployed in a vast range of tasks, from data analysis, automated inference and prediction to the generation of texts and images to robotics. AI applications have left research laboratories and entered our social world, and are being deployed, for instance, in recruiting, lending, law enforcement, medical diagnosis, policymaking, searching for, targeting and generating information, driving autonomous cars and controlling industrial robots. AI opens vast opportunities for individual empowerment, education and well-being, for social progress and environmental sustainability, while at the same time increasing risks for the autonomy,

dignity and equality of individuals, for their fundamental rights and for the values of democracy and rule of law. The AI Act is the first comprehensive piece of legislation in the world that governs the development and deployment of AI. It prohibits some prejudicial uses of AI, establishes requirements and controls over-high-risk AI systems and requires that AI-generated content can be distinguished from human communications.

Policy priorities

The legislative process, including more than 700 amendment proposals by the European Parliament, led to a hypertrophic document of 144 pages which merges political considerations, statements of legal principles and detailed procedural and technical prescriptions in a complex entanglement. Compliance by its addressees (developers and deployers of AI systems) and application by EU and national authorities and other bodies (standard and benchmark setting and certification bodies) will not be easy and will require cooperation by everyone. Interpretation and implementation must indeed fit the elusive pervasive nature of AI, its distributed development, its duplicitous and unpredictable dynamics, and its global development and user base.

First, AI is elusive since it is difficult to distinguish it from other digital technologies. The wording of the definition in the AI Act,

which points to variable autonomy and possible adaptiveness, provides very limited help in this regard. A crucial issue concerns the extent to which the concept of AI besides machine learning-based systems also covers systems based on human-made knowledge representations. Guidance in this regard will be needed.

Second, AI is pervasive since it is rapidly entering all domains of economic, social and individual life, with transformative effects. The AI Act classifies AI systems devoted to certain uses as high-risk, a classification that has become presumptive in the final version of the Act. Only implementation of the Act, thanks to the work of standard-setting bodies and enforcement authorities, will clarify the criteria for this classification and its implication.

Third, AI is characterised by distributed development as new systems and applications of them may be created in different socio-economic settings, from huge tech companies to SMEs and startups to informal collaborations or individual initiatives. Flexibly adapting the application of the AI Act to these diverse addressees will be a challenging task.

Fourth, many AI technologies, such as image recognition and text generation, are susceptible to double or rather multiple uses, some of them beneficial and others prejudicial to individuals and society. How to prevent

dangerous uses without engaging in excessive surveillance, interfering with private choices and preventing useful developments is a key issue. The possibility of experimenting in sandboxes may contribute to effective solutions if a supporting environment is provided thanks to collaboration by regulators and developers.

Fifth, AI is unpredictable in its dynamic of accelerated scientific and technological development, as has been shown by the recent disruptive emergence of AI systems with a general scope, in particular large language models. Some rules on such systems were introduced in the last phases of the legislative process in a hasty attempt to deal with this unforeseen advance. Responding in a principled and technologically sound way to similar future unexpected developments is a challenge for which regulators should acquire appropriate skills and procedures.

Sixth, AI is a global technology, the development and use of which are spread around the world. We cannot just expect that the AI Act will become a global model similar to the GDPR unless two conditions are satisfied. On the one hand, the AI Act must be interpreted, applied and if necessary modified in such a way that it ensures safety and lawfulness while preserving all the opportunities for beneficial deployments of AI. On the other hand, in EU AI research and commercial development must be supported, so that they catch up with the US and China and provide competitive AI Act-compliant applications for deployers and users.

Fostering democratic reflection on digital transformation

Daniel Innerarity, Lucía Bosoer and Marta Cantero Gamito

At a time when digital transformation has become a leitmotif in all debates about the future of Europe, we should consider whether this transformation is being accompanied by a participatory process of reflection, debate and inclusive negotiation on its meaning and impact.

Challenges ahead

It is widely acknowledged that we should strive for a digital transformation of society. However, it is worth asking whether this overarching goal was preceded and accompanied by a corresponding reflection on what a transformation of this size means and whether we have correctly understood the relationship that exists between technology and society.

The narratives that currently dominate debates around tech – particularly when it comes to AI – tend to consider societies and their people as passive subjects on whom technology impacts, whether in a positive or negative way. Technology is often perceived as an exogenous entity with almost omnipotent power that either presents itself unque-

stionably as the best solution to persistent social problems or that poses an existential threat and that we are totally unable to shape or control in any way.

However, technology is fundamentally a social construct and acts in social contexts. For instance, when we use AI systems we act on and interact with algorithms, and modify and reconfigure them. The social power of algorithms stems from recursive relationships between people and algorithms regardless of how asymmetrical they may be. These are encounters that do not take place in a single direction. People limit and expand the ability of algorithms. If we want to give meaning and direction to the process of digital transformation we need to understand technology and we need to understand society, but most

importantly we must understand how the two interact and the ways in which they are interconnected.

Policy priorities

We are therefore facing the great challenge of how to bring technological development and social realities together. Technology does not prescribe only one possible development. Instead, in its encounter with society it creates a dialogue of options that suggests technological pluralism – multiple ways of viewing technology through its social implementation.

When envisioning Europe's digital and technological future, there are at least two factors that should be ensured: thoughtfulness and inclusion. Successful social transformations are achieved more as a result of a thoughtful and continual process than just through speed. Digital transformation demands a consideration of the problems that exist, the structures that should be digitally transformed and the ways in which different stakeholders should be involved. We must examine the factors that could make the digital transformation slower than ideal and the undesirable effects that could be produced by careless implementation. It is often the case that the imperative to not fall behind makes us value velocity over results, and reaction over reflection. This 'action bias'

leads to adaptation without decision-making, direction without agreement, technology without society.

Importantly, this continual process of reflection and negotiation should be configured in an inclusive fashion. We must keep in mind the heterogeneity of the social groups involved in or targeted by the digital transformation: rural and urban environments, different generations, people with varying educational backgrounds, diverse economic situations and the gender inequalities that condition access to and use of technology. Making the digital transformation inclusive and pluralistic entails not only taking into account the diversity of people that affect and are affected by technology but also bringing them to the negotiation table and ensuring that they inform and shape decision-making processes.

The reason why many transitions in this and other areas have failed can be found in the mechanical and vertical application of new requirements without sufficient debate among the societies they were meant to transform. Resistance to change should not be interpreted as some kind of Luddite reaction. Instead, it often reveals that those who are promoting change have not sufficiently or successfully enabled it, negotiated it or made its advantages clear to everyone. To overcome this, a successful process

of inclusive and participatory governance will include strategies that involve providing clear and accessible information about the benefits and implications of new technologies, actively engaging communities in the planning and implementation phases and addressing concerns through open dialogue and feedback mechanisms.

In the end, the societal transformations that will emerge from AI, blockchain, robotics and quantum technologies, among other developments that we do not yet know about, will be a result of the ways in which these technologies and the practices that emerge from and around them are culturally understood, socially organised and legally regulated. To align technological advances with cultural and social contexts, it is essential to integrate a sophisticated understanding of cultural norms and social structures in their development and regulation. By considering the diverse ways in which technology impacts different communities, policymakers can create more effective and widely accepted regulatory solutions and can put forward different policy directions for technology to address specific societal challenges.

Advancing a human-centric vision of virtual worlds

Natalia Menéndez González

While virtual worlds might transform how citizens experience the world, thus benefiting key societal areas, they also entail numerous challenges to EU rights, values and principles which the existing EU digital acquis and new governance instruments should regulate.

Challenges ahead

The European Commission defines virtual worlds as persistent immersive environments built on technologies such as extended reality (XR) and 3D which allow real-time blending of the physical and digital worlds for a range of uses, including designing, simulating, collaborating, learning, socialising, conducting business and entertaining. Virtual worlds have the potential to provide a great deal of innovative opportunities in several societal domains, such as health, education and culture. However, they also bring a wide range of potential threats.

On the consumer side, it is crucial to consider the impact of virtual worlds on physical and mental health, including risks such as addiction, cybersickness, disturbances in sleep patterns and behaviour manipulation. These concerns are particularly relevant for vulnerable groups such as minors (cognitive development) and women (according to the Europe Institute for Gender Equality, one in 10 women has experienced some form of cyber violence since the age of 15). Furthermore, it is important to study how the digital divide will impact the use of virtual worlds, particularly for elderly people, people with disabilities and people living in remote areas.

On the technical, infrastructure and economic side, virtual worlds pose plenty of challenges: the intersection between virtual worlds and AI in general and generative AI in particular; cybersecurity threats; environ-

mental impacts; the lack of standardisation in the sector; power concentration in the hands of a few big tech providers (usually non-EU companies); issues related to data, consumer protection and intellectual property rights; the impact on employment; and a proliferation of criminal activities. These challenges must be thoroughly addressed as virtual worlds continue to expand.

Policy priorities

The European Commission must assess the extent to which existing legislation can effectively regulate virtual worlds, whether they can harmoniously integrate in the Digital Single Market, or if new legislation is required to guarantee fair competition that maximises the potential of virtual worlds and promotes EU economic development. The guiding principles behind all policy measures regarding virtual worlds should be EU values, general principles and fundamental rights, as expressed, for instance, in EU cultural policies, copyright law and labour law. It is important to create virtual environments in which people feel comfortable, confident and empowered, and where their rights as users, consumers, workers and creators are respected.

To achieve this, in the first place the European Commission should focus on providing individuals with the fundamental abilities to navigate virtual worlds and raise European citizens' knowledge of responsible use in these digital areas, particularly by children. In this regard, educational programmes should be established to help children and young people adapt to technological changes and adopt a healthy balanced approach that combines traditional social interaction with time spent in virtual environments. In addition, parents should be provided with the tools they need to supervise their children and make informed decisions about their involvement in the virtual environment. It is also important to monitor addictive and deceptive design patterns ('dark patterns'), and age-appropriate design and parental control mechanisms to protect children. This includes monitoring the exposure of children to abuse, harassment and bullying, and to violent, sexist, racist and pornographic material. Finally, virtual worlds should be made open, inclusive and accessible (in compliance with the European Accessibility Act and the Web Accessibility Directive), and increase involvement by individuals with disabilities.

Second, the European Commission should prioritise the creation of a level playing field that encourages the growth of European small and medium-sized businesses, the creation of competitive European corporations and the development of decentralised and interoperable ecosystems with neutral costs for consumers. To do this, it will be essential to build

new 5G infrastructure and modernise existing infrastructure, particularly in rural areas.

Third, the Commission must carefully monitor the data protection implications of user-generated content and the processing of sensitive data such as biometric and behavioural data, emotional reactions and haptic information. The need for user identification (through the European Digital Wallet) in virtual worlds should be considered, while also recognising that in some instances anonymity may be preferred.

Finally, it is essential to enhance consumer understanding of the environmental impact and sustainability of new technologies. Efforts should be made to expedite and reward technical improvements that lower energy consumption and the environmental footprint of activities related to the creation, use and development of virtual worlds, including enhanced recycling processes and the adoption of renewable energy sources.

Regulatory sandboxes might be a valuable regulatory tool to advance a human-centric vision of virtual worlds. This effort should be preceded by international debates to foster coordination with diverse stakeholders, including consumer groups and other civil society organisations.

Governing blockchain technologies

Morshed Mannan and Primavera de Filippi

In order to reduce legal and regulatory uncertainty in the crypto ecosystem, the European Commission should recognise 'regulatory equivalence' and pay close attention to the dynamics of blockchain network governance.

Challenges ahead

The European Union has engaged in several recent reforms of the regulation of the 'crypto ecosystem,' from updating anti-money laundering and counter-terrorism financing rules to introducing the new Markets in Crypto Assets Regulation (MiCA) for businesses that provide the ecosystem with services. The European Commission had an integral role in stewarding these legislative changes and developing a FinTech Action Plan, which aims to scale up innovative business models in Europe and promote the uptake of blockchain technologies. Despite these developments, the crypto ecosystem is subject to significant regulatory uncertainty, which hinders adoption and stymies innovation in this space in the EU.

The MiCA Regulation, for example, does not cover several types of activities and transactions that are common in this ecosystem. For instance, the regulation does not cover crypto assets that are 'airdropped' into wallet addresses for free, which enable users to access existing goods or services, or those that are automatic rewards for mining or validating activity (Art. 4(3), MiCA Regulation). Relatedly, 'fully decentralised' crypto-asset services are not included (recital 22, MiCA Regulation). These are all significant activities in the ecosystem but the rules of the game are unclear.

Given the recent prosecution of a software developer in the Netherlands for purportedly facilitating money laundering with their work, and the lack of guidance on how decentralised autonomous organisations (DAOs)

will be legally recognised in EU jurisdictions, the risks of criminal liability and unlimited financial liability can deter the development of open-source software necessary for a flourishing crypto-ecosystem.

Policy priorities

We suggest one possible pathway for the European Commission to simultaneously address policy imperatives while retaining the distinct features and benefits of 'fully decentralised' technologies: by recognising regulatory equivalence. As opposed to 'functional equivalence' (which means extending the scope of the law to technologies that it does not explicitly cover but that fulfil the same functions as those that it does), regulatory equivalence means legislators and policymakers recognising that the technological guarantees provided by a new technological artefact can achieve similar policy objectives to existing legal formalities, and might therefore be regarded as equivalent for the purposes of regulatory compliance.

The COALA DAO model law is a practical example of regulatory equivalence. Instead of requiring DAOs to be retrofitted into existing corporate legislation, the model law seeks recognition of DAOs as new corporate entities distinct from existing legal structures. It bestows the privileges of legal personality and limited liability on DAOs if they satisfy the policy objectives that corporate formation requirements serve (e.g. publicity, transparen-

cy, certainty) through technological means. Therefore, instead of requiring DAOs to be registered in a particular state jurisdiction and to comply with regular filing requirements, the model law only requires DAOs to have a unique public address on a public permissionless blockchain through which their activities can be monitored, and bylaws that are comprehensible to laypersons. DAOs that meet these formation requirements are considered to have legal personality. Jurisdictions like New Hampshire and Utah have substantially adopted the model law, in particular by incorporating these formation requirements, thereby taking significant steps towards recognising the regulatory equivalence of these guarantees with local policy aims.

Overall, however, whether the technological guarantees provided by blockchain technology can be regarded as sufficient to qualify as an alternative means of regulatory compliance ultimately depends on the underlying governance of these networks. Both 'on-chain' and 'off-chain' governance have crucial roles to play in the operation of blockchain networks, and only careful analysis of the underlying governance dynamics can reveal whether one can actually rest assured that the network will operate as expected. These issues are at the core of our ERC-funded project 'BlockchainGov' and are synthesised in our two most recent publications: Blockchain Governance (MIT Essential Knowledge) and the Blockchain Governance Cookbook.

Unlocking opportunities and addressing risks in digital finance

Thorsten Beck

In the area of digital finance, the opportunities and risks arising from artificial intelligence have potential to dominate the policy agenda in the next few years.

Challenges ahead

Much progress has been made in the area of digital finance in Europe in the last five years. Specifically, critical legislation has been passed, including the Markets in Crypto Assets Regulation (MiCA) and the Digital Operational Resilience Act (DORA), and a proposal has been made on distributed ledger technology (DLT). In addition, a package on artificial intelligence came into force on 1 August 2024, although the majority of its rules will only start to apply in August 2026.

However, one of the main challenges is the rapidly changing nature of digital finance, with legislators facing an almost impossible task to keep up with developments in technology and the market. In addition, new products and trends can spread much more quickly due to the influence of social media.

The introduction of the digital euro, a *de facto* euro area instant payment system, has made progress. A digital euro legislative framework (Single Currency Package) has been put forward and the European Central Bank is working on implementing the digital euro. However, the use of the digital euro has to be monitored carefully, partly because it constitutes a substitute for bank deposits and can have disruptive effects on banking stability.

Finally, AI has the potential to be truly disruptive in the financial sector and applications of it have to be carefully monitored.

More generally, an increasing use of technology, including AI, combined with a political-cultural division, potentially leads to an increasing share of the population self-excluding from the formal financial sector.

Policy priorities

One important policy area in the near future is the role and impact of artificial intelligence. The opportunities and challenges arising from AI are developing rapidly as the technology is progressing swiftly. On the one hand, there are opportunities for both market players in the financial system and regulators and supervisors. The emergence of RegTech, SupTech and ResTech are clear indications that regulatory and supervisory authorities are trying to benefit from the new opportunities that AI offers. On the other hand, the use of AI in the financial system brings new risks and challenges. It can lead to herding trends across financial institutions and market players. It can make the financial system more vulnerable to cyber- attacks and computing outages. More active supervision is needed, both in normal times and also in the light of how financial institutions and market players react in crisis situations caused by AI.

This is primarily a policy priority for regulatory and supervisory authorities, but policymakers need to ensure that these authorities have sufficient tools and resources to carefully monitor the system. They also need to ensure access by regulatory and supervisory authorities to the necessary data to fulfil these monitoring mandates.

The security of digital infrastructure cannot be completely left to the market. Tackling digital fraud highlights the crucial role of EU regulation in ensuring that digital operators provide their customers with a cyber-secure environment. This will also be a challenge for the about-to-be-established Anti-Money Laundering Authority.

Progress in digital innovation provides opportunities but also poses challenges to financial literacy and inclusion. Despite positive trends, the boom in digital financial services has led to increasing incidents in the EU linked to fraud, over-indebtedness, cyber threats and discrimination. Overall, the digitalisation of finance has facilitated easier access to financial products, yet it has concurrently exposed consumers to unfamiliar and rapidly evolving risks.

Digital financial education is therefore an important policy area. The two OECD-DG FISMA (Directorate-General for Financial Stability, Financial Services and Capital Markets Union) financial competence frameworks are just the start of a much longer process. All the member states must do more, namely develop policies and initiatives targeting children of early schooling age and adults who are engaged in their professions.

These policy priorities cannot necessarily be addressed with legislation, but instead can be with joint efforts by the European Commission, the member states, regulatory and supervisory authorities, and the financial industry itself.

04

Media and Democracy

Rebalancing powers: A holistic strategy to revamp EU platform regulation

Elda Brogi

The EU must update its platform regulation from a constitutional perspective to safeguard fundamental freedoms, address regulatory inconsistencies and ensure that interpreting democratic values is not left to private adjudication.

Challenges ahead

A freedom that can only be exerted by a few is no longer a freedom; it is a power. The European Union is often praised for being at the forefront in setting stringent regulations to curb the power of big tech companies. Indeed, regulations like the General Data Protection Regulation, the Digital Services Act and the Digital Markets Act reflect a proactive stance in legislating on the imbalance between big tech, users and states, which contrasts with the US *laissez faire* approach. EU regulation aims to define the boundaries of these big companies when it comes to protecting personal rights, ensuring a safer online space and boosting openness and competition in digital markets. The so-called 'Brussels effect' serves as a safeguard to protect EU internal standards from being diluted by market globalisation. However, despite these efforts, the EU approach can be seen as largely defensive rather than structural, and it relies too much on the attractiveness of the EU market rather than on innovation.

The European Union strategy regulating big tech has some shortcomings, as large platforms exert influence over media and public discourse. The current regulatory (mostly co-regulatory) framework laid down in the DSA, for instance, imposes duty-of-care obligations on very large online platforms in key areas, such as assessing systemic risks

stemming from their services, including risks to freedom of expression, media freedom and media pluralism (Art. 34 DSA), and implementing measures to mitigate them (Art. 35 DSA). As a result, interpreting freedoms and fundamental principles in the online environment will increasingly be up to very large online platforms and to mere internal auditing. Implementing the DSA, in this sense, could lead to a privatisation of the interpretation of freedoms and fundamental principles, in the long run potentially changing the nature of freedom of expression, media freedom in particular, and how and by whom it is adjudicated.

In addition, all the EU digital legislation, even though ambitious and necessary, suffers from inconsistencies and overlaps that weaken its effectiveness. Moreover, the cost of adhering to these regulations is substantial, which affects not only the platforms themselves but also the institutions tasked with enforcement. Regulatory authorities and other bodies that are involved in digital governance must develop the expertise and technological tools needed to effectively oversee sophisticated digital ecosystems. This not only challenges the efficacy of current regulations but also raises questions about the long-term sustainability of this regulatory approach.

Policy priorities

Constitutional standards and case law already delineate the boundaries of free speech, and they should remain the cornerstone of any regulatory efforts. The accession of the EU to the European Convention on Human Rights (ex Art. 6 TEU) could provide even clearer standards on protecting human rights. By anchoring regulatory measures in established principles, the EU can ensure that efforts to control digital platforms do not inadvertently suppress lawful free speech or impose excessive limitations, for instance in the guise of fighting disinformation.

To build a more resilient media landscape, the EU must consider betting more on digital innovation while also investing in structural and 'constitutional' interventions to support a thriving and innovative media sector that can serve as an effective antidote to the opinion power of platforms. This involves not only providing occasional economic support but also making systematic investments in the media sector, exploring alternative media business models that can reduce reliance on big tech platforms and creating models that sustain public interest journalism without commercial pressure. In addition, the EU should think 'more constitutionally.' The approval of the European Media Freedom Act was a symbolic and normative achievement as it underscores – with its very

existence – the constitutional importance of the news media as the 'fourth estate.'

Along these lines, public service media (PSM) should also receive support to adapt to the digital age. <u>Similarly to what has been proposed in relation to the BBC</u>, the EU should work to ensure that independent PSM are detached from mere market considerations and even 'constitutionalised,' recognising them as a 'necessary and permanent part of a functional democracy.'

Even fair taxation of big tech aimed at ensuring that these platforms contribute to supporting policies linked to the digital economy, <u>such as media support</u>, can be seen as a 'constitutional' measure, contrasting with the scattered regulatory measures in each regulation that require platforms to cover expenses related to implementing the acts themselves.

Power-sharing is a prerequisite for the rule of law and a democratic society. This principle is especially salient in the case of big tech platforms, given their significant degree of market power and control over public opinion. Therefore, also at the international level the European Union should promote stricter standards on platform governance transparency and on political conflicts of interest. Such measures can help protect the digital space from being co-opted by actors whose interests are at odds with both public welfare and democratic values.

Sustaining independent and pluralistic media in the information era

Roberta Carlini

Following the digital disruption of the legacy media business model, the long-term sustainability of independent journalism and pluralistic media remains uncertain. The European Commission should aim to restore fair economic relationships between content creators and digital platforms, foster market plurality and introduce measures to finance journalism as a public good.

Challenges ahead

In the first quarter of the twenty-first century, two major transformations have impacted the media ecosystem and disrupted the media economy. The first is platformisation. The rise of digital platforms as news intermediaries has jeopardised the economic sustainability of the media and changed how people access information. While platformisation has created new opportunities it has also created new threats to media pluralism, the most significant being to the very survival of a pluralistic offer of independent professional information. The second major shift is the rise of artificial intelligence. The development of generative AI systems, in particular, is changing how news is produced and accessed, representing an even more significant transformation that could accelerate pre-existing trends (i.e. the decreasing relevance of professional media as information sources, and the dominance of tech companies in the online advertising market). Because of the high value of media content for AI developers, generative AI could be a game-changer in the relationships between tech companies and media providers (and more generally content creators).

The future of journalism is not just a concern for journalists and media organisations; it will play a crucial role in shaping the future of an informed public sphere in European democracy. The main challenge moving forward is to harness the enormous potential of digital innovation to increase both the supply of, and access to, diverse and independent information. In its previous mandate, the European Commission opted to regulate the digital sphere with a human-centric approach. The specific challenges now lie in implementing and enforcing new rules, many of which could impact media pluralism – particularly the economic relationships between publishers and platforms (data sharing obligations in the DMA, EMFA sections 4-5-6), copyright protection in the AI era (the interplay between copyright laws and AI Act, Art. 53), and safeguarding independent media in pluralistic markets (EMFA). Moreover, it remains uncertain whether these measures will be sufficient to address the market failure in financing journalism, or if direct financial support from the public sector will be necessary.

Policy priorities

One of the key priorities for the new European Commission should be to restore fair economic relationships between content creators and digital platforms, and create a level playing field in the media market. The tradi-tional advertising-financed media business model is gone for good, and restoring it would not be realistic given the enormous competitive advantage of targeted advertising offered by platforms in the search and social media markets. Nonetheless, abuses of market power in the online advertising sector can be sanctioned and addressed using traditional competition law tools, as recent cases have demonstrated. In addition, the Commission and the member states should be vigilant in overseeing the implementation of the DMA data sharing obligations for digital gatekeepers. Effective enforcement of these obligations could counterbalance information asymmetries and help media providers receive a fair share of the value created in the advertising market.

Restoring a level-playing field cannot be achieved without properly measuring attention markets. The main information asymmetry, which is not addressed by the DMA obligations, relates to audience measurements in the digital media environment. Opacity of systems and methodologies disadvantages the weakest players in the market – creators and media content providers. Article 24 of the EMFA addresses this issue by calling for development and standardisation of transparent audience measurement systems. The European Commission, the new European Board for Media Services and national competent authorities should guarantee the effecti-

veness of Article 24, as implementing it is a precondition for the proper functioning of markets and for the very possibility of measuring opinion power and evaluating the risks of concentration (see below).

Achieving fairness must also include initiatives to ensure appropriate remuneration of professional journalism. The implementation of Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market has not solved the issue of fair compensation for authors, journalists and media organisations whose content is monetised by digital intermediaries. While some agreements to compensate media providers have been concluded, they are limited to the mainstream media in the main national markets, and they are not transparent.

Another issue lies in the fragmented regulations that have emerged at the national level as a result of the transposition of the directive on copyright. These national rules fall short of adequately protecting authors and risk hampering innovation by tech companies. Moreover, the development of generative AI models has initiated 'a new battle for copyright' involving different players and dynamics. On a positive note, the AI Act introduces some obligations for general purpose AI models related to copyright protection. In implementing the AI Act, particular attention should be paid to harmonising copyright obligations, developing technical standards for the reservation of rights by right-hol-

ders (opt-outs) and incentivising collective negotiations with the aim of including all the diverse and emerging media outlets and organisations.

Besides ensuring fairness in relations between content creators and platforms, the new Commission must also foster market plurality by introducing and/or strengthening measures to tackle the concentration of media ownership and protect editorial independence. Article 22 of the EMFA introduces a specific assessment of the impact of concentrations in the media market on media pluralism and editorial independence. The main challenge ahead is effective implementation of this provision by the member states, which would lead to a so-called 'media pluralism test' in the single media market. Success of this provision will also depend on the abovementioned efforts to satisfactorily measure attention markets, in particular 'effects on the formation of public opinion' in the digital environment, as stipulated in Article 22(2)(a) of the EMFA. To assess these effects it is essential to understand media consumption habits, not only in terms of the media that people use to inform themselves but also how they access it.

Regarding assessing the impact of concentration on editorial independence, particular attention should be given to the characteristics of merged entities and guarantees related to editorial independence.

Funding journalism as a public good by incentivising public and private investment in the journalism of the future should be another key priority. Public support for private media and public financing of public service media should be reconsidered and reformed to incentivise media innovation and resilience in the digital ecosystem. At the same time, stronger measures are needed to prevent political capture of the media, especially considering growing concerns regarding this issue in many EU member states.

The EU should also consider strengthening its financial support for media pluralism by creating an EU fund for independent journalism. This fund could be financed using a portion of the revenue generated by implementing a new digital global minimum tax.

Integrating the media in EU anti-disinformation policy

Iva Nenadić

As EU policy against disinformation enters a more mature phase, there is a need for a constructive review of the approach taken so far, with a stronger focus on integrating media and journalism in the framework designed to safeguard democracy and citizen access to accurate information.

Challenges ahead

One of the most notable policy areas in the previous European Commission's mandate was the effort to combat disinformation, particularly widespread dissemination of it on and by digital platforms. This policy began to take shape in 2018 with the introduction of the Code of Practice on Disinformation, a self-regulatory initiative involving leading technology companies and representatives of the advertising industry. From its inception, the code focused on five key commitments: cutting financial incentives for disinformation purveyors, ensuring transparency in political advertising, reducing manipulative behaviour, empowering users by increa-

sing transparency in recommender systems and facilitating access to platform data by researchers.

The Commission policy against disinformation also supported a growth in fact-checking organisations and networking among them, fostering cooperation by them with platforms to detect and address disinformation. This was further institutionalised in the 2022 Strengthened Code of Practice on Disinformation, which aimed to resolve the shortcomings of the first version and integrate the code in the broader EU regulatory framework, including the Regulation on the Transparency and Targeting of Political Advertising and the Digital Services Act.

The updated code has expanded scope of formalising platform cooperation with the fact-checking community, including a financial framework for this collaboration. Many fact-checkers, along with other organisations involved in addressing disinformation, have since become signatories of the code. As the policy enters a more mature phase, it presents an opportunity for a constructive review of the approach taken so far and for consideration of future steps, particularly regarding the lack of integration of media and journalistic organisations in the framework.

Policy priorities

Media pluralism is not only a core democratic value but it is also a critical enabler of other fundamental rights, such as freedom of expression and access to accurate information. It has always been essential to safeguard the integrity of democratic discourse by ensuring representation of diverse viewpoints, fostering informed public debate and holding those in power accountable. In today's information environment, in which information overload and various possibilities for generating and amplifying manipulation pose systemic risks, credible reference voices are more crucial than ever. Quality independent media and journalism serve as key antidotes to disinformation.

Unlike fact-checking, which primarily debunks misleading content already circu-

lating in the public space, with professional comprehensive reporting quality media enhance the ability of society to resist manipulative narratives. In contrast, propagandistic outlets and malicious actors that disguise themselves as news media not only spread disinformation but also cause structural harm by eroding trust in the media and undermining the integrity of the information environment. Because of this profound role that news media play regarding disinformation, a comprehensive EU policy against disinformation should give them at least the same prominence as fact-checking organisations.

The commitments adopted and implemented under the Code of Practice on Disinformation include actions such as promoting and demoting content based on its assessed trustworthiness. These interventions, along with other changes to platform content moderation and prioritisation policies, can significantly impact the visibility, reach and financial viability of media content. Platforms have become the primary gateways for access to news and information, acting not as neutral distributors but as commercial entities that shape the information environment with their recommender systems and content policies. As the Code of Practice on Disinformation adds significant input to these content policies, media and journalists should be at the table when they are being discussed.

Better integrating media and journalism in this framework is even more important as the Code of Practice is transitioning into a co-regulation under the Digital Services Act, and is thus becoming a tool for the compliance of very large online platforms with the obligation to assess and mitigate the systemic risks posed by disinformation. Disinformation is of concern in two of the four broad categories of systemic risks covered by the DSA: it threatens civic discourse and electoral processes; and it undermines fundamental rights such as freedom of expression and access to (accurate) information. Any actual or foreseeable negative effects on media freedom and pluralism are also considered a systemic risk in the DSA. These negative effects may arise from content moderation policies of large platforms which, in an effort to reduce disinformation, also limit the reach of political and media content. This is another reason why it is important for the media to be among the anti-disinformation policy instruments.

Another point for the European Commission to consider in a review of the current EU approach to tackling disinformation is that of broader unintended consequences that may arise from separating fact-checking from media and journalism. Encouraging platforms to cooperate with fact-checking organisations without integrating the news media in this collaboration and revenue stream can have significant consequences for the latter and for democratic discourse overall. While there is a need for specialised tech-savvy fact-checking, given the complexity of the information environment and the shortcomings of some of the news media in this area, it is in the interest of the public and healthy democracy for these organisations to collaborate rather than separate.

05
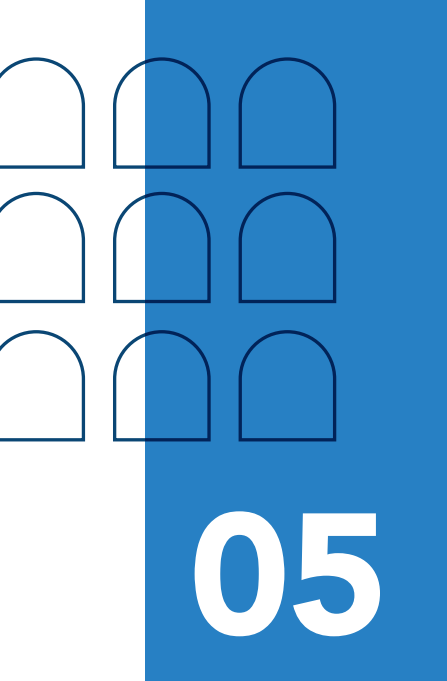
Data

Operationalising European data law

Thomas Streinz

The Commission should prioritise implementation, coordination, monitoring, re-evaluation and eventual recalibration of the burgeoning European data law.

Challenges ahead

The previous European Commission (2019-2024) proposed a flurry of legislation in the digital domain and most of it was enacted: the Data Governance Act, the Digital Services Act, the Digital Markets Act, the Data Act and of course the much-celebrated Artificial Intelligence Act. Political agreement on a regulation for a European Health Data Space was reached. All these laws can be understood – to varying degrees – as 'data laws' and as such they need to navigate their relationship with the EU landmark data protection law, the General Data Protection Regulation (GDPR). In some ways, the GDPR represents a cautionary tale about the difficulty in shaping the digital reality of Europe with law, when most digital infrastructure is actually being developed elsewhere. However, it is not clear whether this is ultimately just an enforcement problem or a conceptual problem at the heart of European data policy.

As the new European data laws operate with conceptions of data that arguably depart from the traditional focus on 'personal data' protection and are to be implemented by a broad array of supranational, national and local institutions, coordination is likely to emerge as a major challenge. But how are we going to know what works and what does not? What are the normative benchmarks for evaluation if different European data laws ultimately advance different interests? How can the EU's experimentalist approach to data law and policy be operationalised effectively?

Policy priorities

If EU data law is meant to shape the socio-technical reality of the European data economy, it needs to be implemented effectively. Effective implementation requires more than investment in public and private enforcement capacity. The various institutions that are called on to implement the various European data laws will need to find ways to productively communicate and collaborate with one another. Internally, the various Directorates-General that are responsible for the different data laws will need to coordinate more closely if European data law is to advance a coherent European data policy. Externally, the new European Data Innovation Board (EDIB) could be developed into an important venue in which data law exchanges take place. However, to be effective the EDIB is likely to require significant investment in the prerequisite infrastructure for data gathering, information-sharing and communication.

The EU attempt at (re)shaping the European digital economy with law can only succeed if law on the books is turned into law in action. The Commission should invest in its monitoring capacity to continually learn about the uptake of European data law on the ground. Are novel data sharing infrastructures emerging as foreseen by the Digital Governance Act? Which businesses use the new data portability rights created by the Data Act? Are vetted researchers gaining access to better platform data thanks to the Digital Services Act? Which search engines are benefiting from mandatory access to search data from gatekeepers under the Digital Markets Act? Does the AI Act affect the data governance practices of AI developers or are they shifting towards developing (supposedly) not-high-risk AI?

These questions and many more can only be answered effectively if the Commission invests in fundamentally improved monitoring capacity. The (re)evaluation clauses routinely contained in European legislation are rendered moot if the infrastructure for continual data-based evaluation is lacking. The Commission should cooperate with European universities to develop such infrastructures as soon as possible to facilitate constant, rigorous and theoretically and empirically grounded evaluations of European data law. Future European data laws should lay the foundation for such infrastructures already in the legislation itself. In the short term, however, the priority should not be new legislation but implementation, coordination, monitoring and re-evaluation of existing law. Finding out what works and what does not and recalibrating the legal regime as necessary should be the Commission's top priority in the field of European data law and policy.

Safeguarding personal data and empowering individuals in the modern digital world

Danielle da Costa Leite Borges

Data protection policies in the next decade should focus on empowering individuals with digital skills to better exercise their digital rights while also equipping national data protection authorities with the tools and resources necessary to hold digital actors accountable.

Challenges ahead

Since 1981, when the Council of Europe opened Convention 108 for signature, protection of personal data in the EU has significantly evolved. The consolidation of rights in the Data Protection Directive in 1995 was then expanded and strengthened with the General Data Protection Regulation, marking an important step towards a human-centric approach to technology and providing a compass for the use of technology in the EU digital transition.

Since the entry into force of the GDPR in 2018, the complex reality posed by our hyper-connected world and the rapid progress of data processing technologies have added new challenges to data protection regulation. In particular, the scale and impact of data processing activities, now made possible by big data components and processors, is reaching levels previously unimaginable. Artificial intelligence learning systems are increasingly sophisticated and capable of searching and integrating large data sets in order to more accurately predict future events, activities and behaviour, and recognise correlations. While data processing activities using AI systems provide opportunities for social knowledge and better governance, enabling automated decision-making in domains that require complex choices and delivering more precise

and impartial results, they also present risks to individuals and to society at large. On the one hand, the use of AI learning systems may affect individuals due to persistent monitoring and potential targeting in different spheres of their lives. On the other hand, even if these learning systems do not directly interfere with data protection, the behavioural data they produce through search queries and clicks, for instance, can be misused by corporations, digital elite members and governments to change the balance of power in society.

From a data protection perspective, there is no simple solution to this issue. The human-centric perspective that permeates EU policies in this area has considerably focused on rights and exercising them, while overlooking the conditions and requirements necessary to exercise these rights effectively. In this context, EU citizens and society need to be digitally well equipped to face the challenges of the next digital decade.

Policy priorities

The 2020 European Data Strategy recognised that growing data volumes and technological changes require, among other things, greater respect for privacy and data protection laws in order to enable functioning of the data economy in the bloc in the years to come. One of the pillars of this strategy was empowering individuals to exercise their rights, including improving their digital skills, considering the existence of data literacy gaps in the workforce and the EU population, especially among certain social groups such as the elderly. In effect, in terms of data governance regulation, the EU has over the last five years taken several steps towards achieving a data-driven economy, such as adopting the Digital Services Act, the Digital Markets Act, the Data Governance Act, the Data Act and the Artificial Intelligence Act. These pieces of legislation aim, among other things, to empower individuals. The DMA, for instance, mandates that consent be the sole legal basis for processing personal data by platforms designated as 'gatekeepers,' particularly for the purpose of data combination and cross-use in the ecosystems of platforms. Considering that consent serves as a mechanism to reinforce the choice and control of data subjects, Article 5(2) DMA is an example of the EU strategy to empower individuals.

However, the improvement in digital skills has not received the same level of attention from EU policymakers and legislators. In fact, a 2024 European Parliament study concludes that no EU legislation addresses the digital divide affecting elderly people. Therefore, improving digital literacy should be a data protection policy priority in the coming years. Individuals will only be able to fully exercise their data protection rights, as set out in the GDPR and other legislation, if they have the

necessary digital skills – skills that will become increasingly important as technology advances and AI systems become more widespread.

While empowering individuals in relation to their data protection rights is undoubtedly an important policy priority, alone it is not sufficient to address the many challenges that lie ahead. Relying solely on strong individual rights and individual responsibility may not effectively achieve the main objective of protecting personal data and may instead reinforce the so-called 'privacy paradox.' Therefore, a second EU policy priority in the area of data protection should be enforcing accountability, a key principle in the GDPR. Achieving a safe data environment for the use of personal data in the EU also depends on the accountability of data controllers and processors, who are in a better technical position to take decisions in relation to the data they process. Holding these actors accountable is essential to achieve a safe trustable data environment and should be seen as a way to create value in the EU data space and open up opportunities for new competitors and innovation.

Accountability, however, requires strengthening the institutions entrusted with the task of holding these actors to account. Hence, the third and final policy priority in this area should be strengthening the role of data protection authorities. This means providing them with the necessary conditions to carry out their tasks and exercise their powers independently, including transparent procedures to appoint their boards and ensuring they have sufficient technical, budgetary and human resources. In addition, enhanced cooperation between these authorities should be encouraged by the European Data Protection Board to promote a more coherent application of data protection rules in the EU. This cooperation should be extended to other national authorities entrusted with overseeing the implementation of related policy areas, to make sense of the various digital regulations that intersect with data protection and to ensure consistent application of them.

www.eui.eu

Co-funded by
the European Union