Centrum für Europäische Politik
FREIBURG | BERLIN

cepInput

No 2 | 2025 14 January 2025

How Europe Can Navigate the Regulatory Tightrope

Trade-Offs and Risks in EU Digital Policy

Anselm Küsters and Cecilia Emma Sottilotta

Source: Figure generated by DALL-E

The recent creation of the post of EU Commissioner for Tech Sovereignty, Security and Democracy underlines the bloc's newfound energy to asserting its role in the global digital landscape. However, this ambition brings with it a complex web of trade-offs that, if unrecognised, pose risks to the EU's future digital policymaking. This policy brief explores and categorises these trade-offs and suggests how to address them.

- EU policy-making by its very nature involves trade-offs. For instance, decisions that aim to strengthen technological sovereignty may hinder market competitiveness or stifle innovation. Failure to recognise these trade-offs can lead to unintended consequences, such as regulatory overreach or reduced cooperation.
- In the absence of technological leadership, there is a critical trilemma between tech sovereignty, security, and democracy, where improving one aspect may compromise the others. We analyse this trilemma for the EU through case studies on privacy vs. innovation in the GDPR, regulation vs. freedom of expression in the Digital Services Act, cybersecurity risks and economic incentives in European ICT development, ethics vs. competitiveness in AI regulation, autonomy vs. cooperation regarding computing infrastructure, and consumer welfare vs. external values in Big Tech competition policy.
- We propose that increased cooperation with international partners and digital diplomacy can help the EU mitigate some trade-offs. Overall, recognising and strategically managing digital policy trade-offs is crucial for the EU to achieve its ambitions for tech sovereignty without compromising its founding principles.

Content

Figures

1 Introduction

Rapid technological advances, coupled with changing geopolitics, have intensified the challenges for the European Union (EU) in governing the digital space. The appointment of a new EU Commissioner for "Tech Sovereignty, Security and Democracy" signals a strategic move to address these complexities. However, this development also highlights a critical issue: the EU's digital policies often involve inherent trade-offs that are not sufficiently recognised or openly debated, which in turn creates regulatory uncertainty and risks. For instance, it is often postulated that detailed, top-down regulations designed to protect citizens might inadvertently hamper the competitiveness of European businesses on the global stage. In a similar vein, efforts to enhance security might infringe on individual privacy rights or stifle civil liberties, conflicting with the EU's core democratic principles.

This cep**Input** analyses these often-unacknowledged trade-offs. By examining specific case studies, we aim to uncover in more detail the delicate balance required between competing objectives and highlight the potential risks of neglecting these complexities. Our analysis covers a number of critical areas in relation to European digital policy, including privacy versus innovation in the data protection rules, regulation versus freedom of expression in platform moderation, cybersecurity risks and economic incentives in European ICT development, ethical standards versus competitiveness in AI regulation, strategic autonomy versus global cooperation in building large-scale computing infrastructure, and consumer welfare versus broader public interests in the context of tech-focused competition policy.

An overarching theme emerges from these case studies. The threats to democracy and security posed by technological advances and digital policies are often multi-causal, thereby defying simplistic causal explanations. This complexity is compounded by the relative novelty of many of the underlying trade-offs, resulting in a lack of long-run empirical data and scholarly consensus. However, this lack of systematic analyses and the open-ended nature of empirical research do not diminish the importance of the impact of technology on democracy and security, nor does it absolve EU digital policy from addressing these concerns. Rather, the protection of fundamental values is an inherently preventive task, necessitating proactive policy measures.

Recognising and addressing the trade-offs in the EU's digital policy is essential to avoiding discretion and enable subsequent policy learning over time while fostering a resilient, innovative, and democratic digital ecosystem in Europe. This challenge is particularly relevant in light of the EU's plans to unify and harmonise digital rules across member states in the next mandate, aiming to simplify the regulatory landscape while maintaining effectiveness. As the new EU Commissioner for "Tech Sovereignty, Security and Democracy" takes office, our analysis suggests that no single policy approach can adequately address all concerns without potentially compromising other important public policy objectives. With this in mind, we suggest – perhaps counterintuitively – that enhanced and strategic cooperation with international partners and digital diplomacy could help the EU mitigate some of the trade-offs.

Building on this motivation, our paper is structured as follows. First, we draw on existing literature and theories to derive a general framework for analysing trade-offs in EU digital policy (section 2). The core of our analysis is devoted to six individual case studies, each highlighting a specific area of EU digital policy where significant trade-offs and resulting risks are evident (section 3). Following these case studies, we turn our attention to the external dimension of EU digital policy (section 4). Here, we explore how partnerships and international cooperation can potentially help address some of the trade-offs identified and offer a path towards more effective policy. Finally, we conclude (section 5).

2 General scheme for analysing EU digital policy trade-offs

The trilemma, also known as the "impossible trinity", is a popular conceptual framework in international economics that highlights the inherent trade-offs policymakers face in managing their economies in an increasingly globalised world.[1] The classic macroeconomic trilemma, first conceptualised by Mundell and Fleming in the 1960s, states that a country cannot simultaneously achieve a fixed exchange rate, a free capital account, and independent monetary policy.[2] According to this theory, policymakers must choose only two of these three objectives, as it is impossible to achieve all three at the same time. There are many historical examples for this type of trade-off: By adopting a common currency, for example, the euro area countries have effectively chosen to have fixed exchange rates with each other and to allow free movement of capital – at the cost of sacrificing independent monetary policy.[3] In a similar vein, Schoenmaker proposed a "fiscal trilemma" that applies specifically to fiscal policy.[4] This trilemma suggests that countries cannot simultaneously achieve financial stability, financial integration, and national fiscal policy. Rey challenged the traditional trilemma by arguing that in a world of high capital mobility, independent monetary policy is possible only if the capital account is managed.[5] This perspective suggests that some trilemmas may evolve over time – in this case turning into a dilemma between monetary policy autonomy and capital mobility. More recently, observers have begun to ask whether a trilemma might also exist in the area of digital policy.[6]

Indeed, tech policymaking is fraught with complex trade-offs, which, if overlooked, can lead to policies that undermine their own objectives.[7] Within the EU, three objectives have been repeatedly highlighted, not least by EU Commissioners during their parliamentary hearings and in recent reports such as those published by Draghi and Letta: economic competitiveness and innovation; security and sovereignty; as well as fundamental rights and social cohesion (Figure 1). The EU aims to be a world leader in digital innovation, fostering an environment in which businesses can flourish and technological advances such as Artificial Intelligence (AI) can be rapidly adopted with plans like the "AI Factories" or

---

1 Joshua Aizenman, Menzie David Chinn, and Hiro Ito, 'The "Impossible Trinity" Hypothesis in an Era of Global Imbalances: Measurement and Testing', *Review of International Economics* 21, no. 3 (August 2013): 447–58, https://doi.org/10.1111/roie.12047.

2 R. A. Mundell, 'Capital Mobility and Stabilization Policy Under Fixed and Flexible Exchange Rates', *Canadian Journal of Economics and Political Science* 29, no. 4 (November 1963): 475–85, https://doi.org/10.2307/139336; J. Marcus Fleming, 'Domestic Financial Policies under Fixed and under Floating Exchange Rates', *Staff Papers - International Monetary Fund* 9, no. 3 (November 1962): 369, https://doi.org/10.2307/3866091.

3 Maurice Obstfeld, Jay C. Shambaugh, and Alan M. Taylor, 'The Trilemma in History: Tradeoffs Among Exchange Rates, Monetary Policies, and Capital Mobility', *Review of Economics and Statistics* 87, no. 3 (August 2005): 423–38, https://doi.org/10.1162/0034653054638300. During the Bretton Woods system (1944 to 1971), countries maintained fixed exchange rates against the US dollar and had monetary policy autonomy, but capital controls were widely used. Maurice Obstfeld and Alan Taylor, 'The Great Depression as a Watershed: International Capital Mobility over the Long Run' (Cambridge, MA: National Bureau of Economic Research, March 1997), https://doi.org/10.3386/w5960.

4 Dirk Schoenmaker, 'The Financial Trilemma', *Economics Letters* 111, no. 1 (April 2011): 57–59, https://doi.org/10.1016/j.econlet.2011.01.010.

5 Hélène Rey, 'Dilemma Not Trilemma: The Global Financial Cycle and Monetary Policy Independence' (Cambridge, MA: National Bureau of Economic Research, May 2015), https://doi.org/10.3386/w21162.

6 José Ignacio Torreblanca and Giorgos Verdi, 'Innovate, Protect, and Influence: The EU's Technology Trilemma and How to Solve It', *European Council on Foreign Relations*, June 2024, https://ecfr.eu/article/innovate-protect-and-influence-the-eus-technology-trilemma-and-how-to-solve-it/.

7 For the trade-offs between competition and innovation in digital markets, see: Avi Goldfarb and Catherine Tucker, 'Digital Economics', *Journal of Economic Literature* 57, no. 1 (1 March 2019): 3–43, https://doi.org/10.1257/jel.20171452. For trade-offs around privacy, competition, and innovation see: Alessandro Acquisti, Curtis Taylor, and Liad Wagman, 'The Economics of Privacy', *Journal of Economic Literature* 54, no. 2 (1 June 2016): 442–92, https://doi.org/10.1257/jel.54.2.442. For trade-offs in AI governance, see: Luciano Floridi, 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU', *Philosophy & Technology* 33, no. 3 (1 September 2020): 369–78, https://doi.org/10.1007/s13347-020-00423-6.

the “Apply AI” initiative. At the same time, it must protect its digital infrastructure and data from external actors to ensure strategic autonomy, e.g. in the cloud space. At least equally important is the commitment to uphold individual privacy, freedom of expression, and other fundamental rights that are deeply embedded in its legal framework and the founding Treaties. In short, official rhetoric strongly suggests that EU digital policy aims to balance competitiveness, sovereignty, and rights.

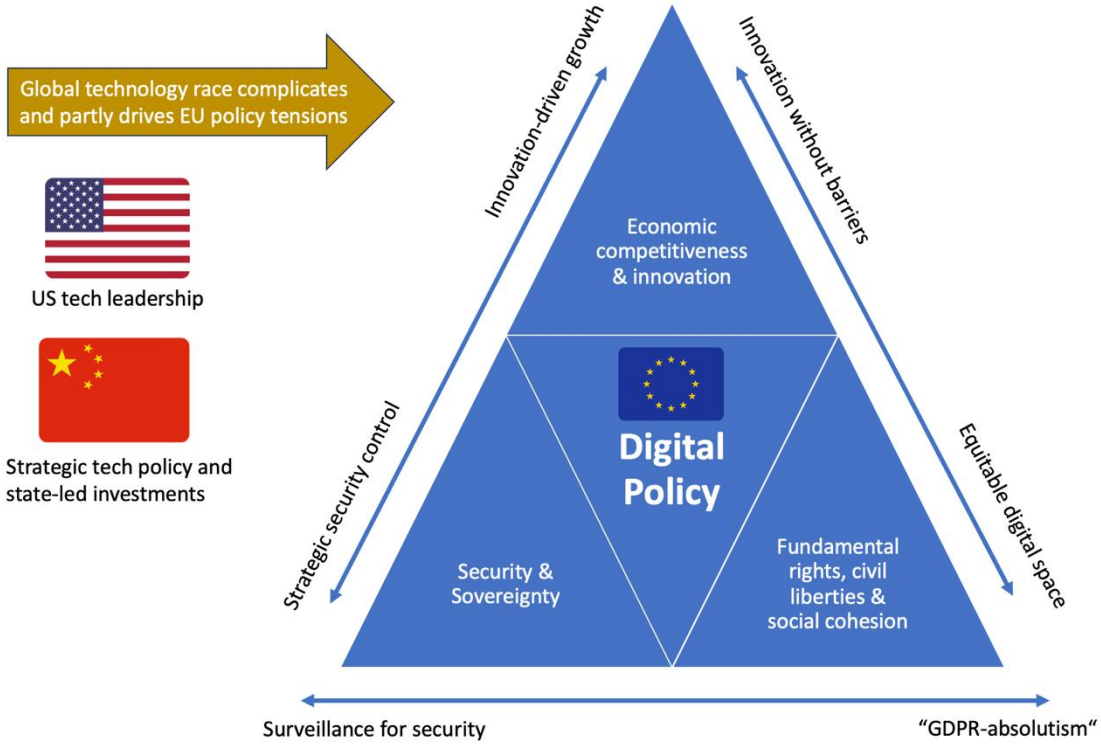
To distinguish the competing three goals at the outset, we offer the following definitions: (1) Economic competitiveness (and innovation): The ability of EU firms (including start-ups, SMEs, and large companies) to innovate and grow in the global digital marketplace, driving economic prosperity. (2) Security (and sovereignty): The protection of critical digital infrastructure, data, and strategic autonomy. Sovereignty encompasses both national security interests and the EU's collective ability to set its own policy directions free from external dominance. (3) Fundamental rights (and social cohesion): Safeguarding individuals’ privacy, freedom of expression, and other legal rights enshrined in the EU Treaties and Charters in the virtual realm, including ensuring equal participation in the digital society. We hypothesise that overemphasis on one dimension often impacts on another.

Is it therefore possible to speak of a digital policy trilemma facing the EU today? In general, many real-world policy trade-offs manifest themselves in pairwise terms. In the macroeconomic context, a trilemma arises when it is *structurally* impossible to pursue all three objectives simultaneously. In our digital policy context, we rather argue that intensifying one objective (e.g., increasing economic competitiveness at all costs) tends to create tensions with at least one of the other two (security/sovereignty or fundamental rights). Over time, a policymaker who tries to preserve strong sovereignty and strong fundamental rights while at the same time pushing for maximum competitiveness is likely to be constrained in at least one area. In contrast to the classic “impossible trinity”, where the choice between two macroeconomic objectives inevitably sacrifices the third, we invoke the term “trilemma” in a more *heuristic* sense: the interplay between the three objectives may become so constraining that prioritising one or two objectives makes it more difficult to fully realise the third. While a more technically accurate label might be a three-goals triangle featuring multiple two-sided trade-offs (Figure 1), the core insight remains: EU digital policymakers must recognise how efforts to support one goal may constrain the others and that prioritising any two objectives often imposes constraints on the third, especially in the context of a global technology race. In this sense, external pressure generated by US tech leadership could be seen as an external factor that further links what might otherwise appear to be separate pairwise trade-offs.

One might thus ask whether the EU’s “trilemma” arises simply because other jurisdictions, notably the US, have chosen a different balance between these three objectives. Of course, the EU’s digital policy challenges do not exist in a vacuum and are shaped by external factors such as US technological leadership and the growing role of China, both of which we discuss below. Decisions taken in jurisdictions with large internal markets and/or global “digital champions” limit the EU’s room for manoeuvre if it is to remain competitive. However, we also stress that to a significant degree, the EU’s policy framework derives from its core values and Treaty commitments, which emphasise fundamental rights, social cohesion, and market integration as core principles. Thus, the specific shape of the EU’s digital policy trilemma partly reflects different societal and legal priorities, but it is also influenced by the reality of US market leadership in technologies such as AI, social media, and cloud computing (which the incoming Trump 2.0 presidency is clearly aware of and seeks to exploit). The latter aspect of the

trilemma implies that Europeans are simply not always free to fully choose according to their societal preferences, a problem that may also arise in other areas of policy making.

Fig. 1: Generalised trilemma in EU digital policymaking



Source: Own Illustration.

To illustrate our three-goals triangle, featuring multiple two-sided trade-offs, consider each side of the "trilemma" in turn (Figure 1). To begin with, the relationship between economic competitiveness (and innovation) and security (and sovereignty) illustrates the first dimension of the EU's trilemma. On the one hand, policies to promote competitiveness often prioritise the creation of an environment conducive to the expansion of businesses and technological progress. This approach typically involves reducing regulatory burdens to allow firms to innovate freely and compete globally. However, this can inadvertently create security vulnerabilities, for instance if not carefully balanced with cybersecurity standards or considerations of supply chain dependencies. Conversely, an emphasis on security and sovereignty might lead to the implementation of stringent cybersecurity measures and data protection protocols to guard against foreign influence and protect critical infrastructure. While these measures increase security, they also increase compliance costs for companies and restrict data flows, potentially hindering the AI-driven growth of EU-based companies. Stricter policies regulating the cross-border movement and domestic use of electronic data significantly hamper the performance of data-dependent firms, with stronger effects in countries with advanced technology networks and for service firms.[8]

Another critical aspect of the trilemma is the interaction between security and fundamental rights. While the EU has progressively integrated fundamental rights into its laws and policies, it lacks a

[8] Martina Ferracane, Janez Kren, and Erik Van Der Marel, 'Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries?', *SSRN Electronic Journal*, 2019, https://doi.org/10.2139/ssrn.3384004.

cohesive framework to make these benefits more apparent to the public.[9] In addition, there are ongoing negotiations on the division of judicial tasks between national and EU courts with regard to the interpretation and enforcement of fundamental rights.[10] Finally, governments seeking to strengthen security and sovereignty often introduce measures such as surveillance or data localisation requirements to monitor digital activities more effectively.[11] While such measures can enhance security, they often come at the expense of individual privacy, which can undermine public trust. However, this trade-off may depend on one's perspective. From an outward-looking perspective, EU sovereignty – particularly vis-à-vis actors such as the US or China – can be reconciled with privacy protection under frameworks such as the GDPR. For example, ensuring that EU citizens' data is stored within the EU strengthens both privacy and sovereignty by allowing member states to implement a collective vision free from external influence. However, from an inward-looking perspective, a focus on surveillance for national security can actually clash with some sort of "GDPR absolutism", as strict privacy laws could hinder data sharing critical for law enforcement. The trade-offs between security, sovereignty, and fundamental rights are thus not absolute, but shaped by broader geopolitical and domestic priorities.

The final dimension of the trilemma is the tension between rights/rules and competitiveness. When economic growth and innovation take precedence, policies tend to favour minimal regulatory constraints, allowing for rapid technological progress and cost-effective solutions while potentially facilitating privacy risks or socio-economic inequalities. Conversely, prioritising fundamental rights emphasises the creation of an equitable digital space but may introduce strong regulatory barriers that affect the agility of digital businesses. Bradford's theory on the "Brussels Effect" explains how EU regulations influence global markets while balancing competitiveness with ethical governance principles.[12] In the technology field, some have even argued that the EU's ability to project power stems not only from its market size, but also from its consensual, inclusive policy-making, which ensures legal certainty and credibility, thus influencing other states to adopt the EU's high standards of regulation.[13] Lately, however, some have cautioned that the Brussels Effect is at risk of gradual erosion over the coming years, not least due to changing geopolitics.[14] Even in the case of the widely cited DSA and AI Act, Šonková finds that there are limitations to achieving a Brussels Effect.[15] To address this tension, the EU has recently sought to refine its regulatory strategy through several mechanisms, including: the innovation principle, which aims to ensure that new policies take into account their potential impact on innovation; regulatory budgeting, a system of capping or offsetting regulatory costs aimed at minimising

[9] Israel Butler, 'A Fundamental Rights Strategy for the European Union' (Open Society Foundations, 2014), JSTOR, http://www.jstor.org/stable/resrep43002.

[10] Aida Torres Pérez, 'The Federalizing Force of the EU Charter of Fundamental Rights', *International Journal of Constitutional Law* 15, no. 4 (3 November 2017): 1080–97, https://doi.org/10.1093/icon/mox075.

[11] Rocco Bellanova, Helena Carrapico, and Denis Duez, 'Digital/Sovereignty and European Security Integration: An Introduction', *European Security* 31, no. 3 (3 July 2022): 337–55, https://doi.org/10.1080/09662839.2022.2101887.

[12] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (New York: Oxford University Press, 2020).

[13] Annegret Bendiek and Isabella Stuerzer, 'The Brussels Effect, European Regulatory Power and Political Capital: Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate', *Digital Society* 2, no. 1 (April 2023): 5, https://doi.org/10.1007/s44206-022-00031-1.

[14] Andrea Renda, 'Leveraging Digital Regulation for Strategic Autonomy', March 2022, https://feps-europe.eu/publication/853-leveraging-digital-regulation-for-strategic-autonomy/.

[15] Markéta Šonková, 'Brussels Effect Reloaded? The European Union's Digital Services Act and the Artificial Intelligence Act', EU Diplomacy Papers (College of Europe, Department of EU International Relations and Diplomacy Studies, April 2024), https://www.coleurope.eu/sites/default/files/research-paper/EDP_4_24%20Sonkova.pdf.

unnecessary burdens on business; and the introduction of regulatory sandboxes, i.e. controlled environments that allow firms to test technologies or business models under regulatory supervision.[16]

Crucially, ignoring these trade-offs carries significant risks. Without recognising the inherent tensions described in our trilemma, EU digital policies can become incoherent, contradict each other, and lead to ineffective or even counterproductive outcomes. These types of constraints due to conflicting goals have plagued not only the EU's governance approach to the internet[17] and cyber-security rulemaking,[18] but also non-digital policy fields like neighbourhood policy.[19] A prime recent example of this delicate balance can be seen in the development of the Digital Markets Act (DMA), where competing economic ideas of political actors, namely "market-correctors", "market-busters", and "market-directors", counteracted each other.[20] Moreover, an insular focus on a single aspect can reduce the EU's ability to shape global digital standards and norms through a more holistic overarching strategy, ceding leadership to other geopolitically strategic actors with more long-term thinking, such as China.

As the EU grapples with its digital policy trilemma, it is important to note that other major global players face their own complex trade-offs in regulating the digital sphere. In China, the regulatory landscape resembles, according to Zhang, a high-wire act characterised by hierarchy, volatility, and fragility.[21] This analogy aptly captures the balance Chinese regulators must maintain between fostering innovation, asserting state control, and managing social stability. The hierarchical nature of China's regulatory system means that decisions often cascade from the top, leading to rapid policy changes. This volatility can create uncertainty for businesses, but also allows for rapid adaptation to emerging challenges, Zhang argues. However, the fragility of the system becomes apparent when conflicting priorities emerge. Unlike the EU's trilemma, China's trade-offs often prioritise state control and economic growth over individual rights. This is, for instance, evident in how China has transformed antitrust into a powerful economic weapon, using it strategically to counter US sanctions and tilt the competitive landscape in favour of domestic firms, while also using it as an instrument of trade and foreign policy.[22]

In contrast, the US has a similarly – or perhaps even more – fragmented regulatory landscape, with significant discrepancies between federal and state approaches to digital policy. This decentralised system allows for greater experimentation and flexibility, as evidenced by California's proactive stance on AI regulation. The state's proposed AI accountability measures and transparency requirements

---

[16] Andrea Renda and Jacques Pelkmans, 'EU Regulation: Hindering or Stimulating Innovation?', in *Handbook of Innovation and Regulation*, ed. Pontus Braunerhjelm et al. (Edward Elgar Publishing, 2023), 263–93, https://doi.org/10.4337/9781800884472.00021.

[17] George Christou and Seamus Simpson, 'The European Union, Multilateralism and the Global Governance of the Internet', *Journal of European Public Policy* 18, no. 2 (March 2011): 241–57, https://doi.org/10.1080/13501763.2011.544505.

[18] Helena Carrapico and André Barrinha, 'The EU as a Coherent (Cyber)Security Actor?', *JCMS: Journal of Common Market Studies* 55, no. 6 (November 2017): 1254–72, https://doi.org/10.1111/jcms.12575; Elaine Fahey, 'The EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security', *European Journal of Risk Regulation* 5, no. 1 (March 2014): 46–60, https://doi.org/10.1017/S1867299X00002944.

[19] Tanja A. Börzel and Vera Van Hüllen, 'One Voice, One Message, but Conflicting Goals: Cohesiveness and Consistency in the European Neighbourhood Policy', *Journal of European Public Policy* 21, no. 7 (9 August 2014): 1033–49, https://doi.org/10.1080/13501763.2014.912147.

[20] Catherine Hoeffler and Frédéric Mérand, 'Digital Sovereignty, Economic Ideas, and the Struggle over the Digital Markets Act: A Political-Cultural Approach', *Journal of European Public Policy*, 22 December 2023, 1–26, https://doi.org/10.1080/13501763.2023.2294144.

[21] Huyue Zhang, *High Wire: How China Regulates Big Tech and Governs Its Economy*, Oxford Scholarship Online Political Science (New York, NY: Oxford University Press, 2024), https://doi.org/10.1093/oso/9780197682258.001.0001.

[22] Angela Huyue Zhang, *Chinese Antitrust Exceptionalism: How the Rise of China Challenges Global Regulation* (New York: Oxford University Press, 2021).

demonstrate how individual states can serve as laboratories for policy innovation. However, this patchwork approach also creates challenges for companies operating across state lines and can lead to inconsistencies in consumer protection and privacy standards. More generally, the US approach to the trilemma often tends to prioritise security over privacy, as evidenced by federal legislation such as the Patriot Act, which has enhanced law enforcement capabilities and counter-terrorism efforts at the expense of robust privacy protections and coherent digital governance. This prioritisation of security and competitiveness leaves gaps in the uniformity of privacy standards that states must attempt to fill. As a result, the US model exemplifies a different set of trade-offs, where the balance between security and privacy tilts in favour of the former, shaped by federal imperatives and state-level innovation.

In contrast to both China and the US, the EU's approach to being a global digital actors stands out because of its unique political structure, economic objectives, and legal framework.[23] As a supranational entity, the EU must balance the interests of multiple member states while striving for a cohesive digital market – which becomes even more challenging during times of multiple crises and populist voting.[24] Balancing the vertical relations between the EU, its Member States, and private actors and the horizontal relations between its multiple institutions and agencies requires a more deliberative and consensus-driven approach to policymaking, which can result in more comprehensive but slower-to-implement regulation. Economically, the EU aims to foster a competitive digital ecosystem while maintaining its "social market economy" model, resulting in policies that seek to balance business interests with strong consumer and worker protection. Legally, the EU's commitment to fundamental rights, as enshrined in the Charter of Fundamental Rights, prioritises privacy and data protection, especially compared to other regions.[25] This combination of factors results in a regulatory approach that needs to be careful in dealing with the digital policy trilemma – as we will show in the next section.

3 Individual case studies

Regulation can generally be seen as a political decision to balance trade-offs. As hypothesised in the previous section, EU digital policy-making is fraught with many such trade-offs, which, if not recognised, can lead to policies that undermine their own objectives. To illustrate and dissect this "trilemma", this section analyses the trade-offs and associated risks for six specific case studies: privacy vs. innovation in European data protection, regulation vs. freedom of expression in platform moderation, cyber-security risks and economic incentives in European ICT development, ethics vs. competitiveness in AI regulation, strategic autonomy vs. cooperation when developing computing infrastructure, and consumer welfare vs. broader public interests in EU competition policy.[26] The aim is to see whether there are structural parallels between these trade-offs in different sub-areas of EU digital policy, or whether the trade-offs take a specific shape (and if so, what factors are driving this).

[23] Elaine Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, Modern Studies in European Law, volume 111 (Oxford ; New York: Hart, 2022).

[24] Frank Schimmelfennig, 'European Integration (Theory) in Times of Crisis. A Comparison of the Euro and Schengen Crises', *Journal of European Public Policy* 25, no. 7 (3 July 2018): 969–89, https://doi.org/10.1080/13501763.2017.1421252; Andreas C. Goldberg, Erika J. Van Elsas, and Claes H. De Vreese, 'The Differential Impact of EU Attitudes on Voting Behaviour in the European Parliamentary Elections 2019', *Journal of Contemporary European Studies* 32, no. 4 (October 2024): 1323–42, https://doi.org/10.1080/14782804.2024.2356643.

[25] Torres Pérez, 'The Federalizing Force of the EU Charter of Fundamental Rights'.

[26] For a similar case study approach, see: Renda and Pelkmans, 'EU Regulation'.

3.1 Data protection: Privacy vs. innovation

The General Data Protection Regulation (GDPR) is a landmark piece of EU privacy legislation, with far-reaching implications for businesses around the world.[27] Implemented in May 2018, the GDPR aims to strengthen individual data rights and harmonise privacy regulations across the EU. While the regulation has been lauded for improving consumer privacy, it has sparked intense debate about its impact on business innovation and competitiveness, particularly for smaller companies and start-ups. The GDPR imposes strict requirements on how companies collect, process, and store personal data, requiring operational changes and compliance investments for many organisations. As a result, several trade-offs between privacy and economic processes related to tech innovation have become visible.

To begin with, the GDPR operates through a multifaceted regulatory framework that combines elements of command and control, design-based, and meta-regulation, as highlighted in a recent study by Martínez.[28]. This approach creates a dynamic system in which data controllers must not only comply with specific rules, but also engage in continuous risk assessment and management. In particular, the regulation's risk-based approach requires organisations to assess the nature, scope, and context of data processing, taking into account the potential impact on fundamental rights beyond privacy. This complexity is compounded by the GDPR's principles of privacy by design and by default, which require the integration of privacy measures throughout the lifecycle of technologies and applications.

Accordingly, implementing GDPR compliance (on part of businesses) is not a straightforward process, as it involves dealing with a spectrum of regulatory modalities. The so-called data controllers must justify their processing activities on at least one legal basis, while also integrating GDPR principles into their technical and organisational processes. The principle of data protection by design, for example, requires anticipating potential data protection risks at the earliest stages of product development. This proactive approach aims to embed privacy considerations at the core of technological innovation, rather than treating them as an afterthought. However, Martínez suggests that this complexity can lead to different interpretations and implementations of GDPR requirements, potentially leading to scenarios of both under-compliance and over-compliance.[29] In some cases, over-compliance or "ultra vires compliance" may occur, where companies implement measures that go beyond the actual requirements of the GDPR.[30] Clearly, unnecessary restrictions on data processing activities limit the development of data-driven technologies and services. More generally, the regulation's emphasis on comprehensive risk assessment and management imposes significant burdens on organisations. As a result, the trade-offs made in favour of risk aversion in the development of the GDPR may have unintended consequences for economic growth and technological progress in the EU.

Having dealt with the legal theory, what is the evidence that this legal complexity and the prioritization of risk aversion over economic imperatives has led to economic disadvantages? Analysing a large sample of companies across 61 countries and 34 industries, Frey and Presidente found that companies exposed to EU markets experienced an average 8% drop in profits and 2% drop in sales following GDPR

[27] Bradford, *The Brussels Effect*.
[28] Alba Ribera Martínez, 'Ultra Vires Compliance as a GDPR Harm' (November 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5008314.
[29] Ribera Martínez.
[30] Ribera Martínez.

enforcement.[31] Notably, the negative impact was particularly pronounced for small technology firms, which experienced almost double the average decline in profits. In contrast, large technology companies appeared relatively unaffected, suggesting that the regulation may inadvertently favour established tech giants over smaller competitors. Research by Peukert et al. sheds further light on how the GDPR has reshaped the digital ecosystem.[32] Tracking over 110,000 websites, the study found a significant reduction in connections to web technology providers post-GDPR. At the same time, they observed an increase in market concentration in web technology services.

Focusing on innovation outcomes, Blind, Niebel, and Rammer examined the impact of GDPR on product innovation among German firms.[33] Their analysis revealed a significant shift from radical to incremental product innovation following the implementation of the regulation. Radical innovation refers to the development of entirely new products that represent a significant departure from existing offerings, typically creating new markets or disrupting existing ones. In contrast, incremental innovation involves modest improvements or adaptations to existing products, i.e., simply enhancing their features or performance. The researchers also note that GDPR compliance efforts prompted firms to fundamentally reorganise their data management practices. The resources required to comply with the regulation appear to have limited companies' ability to develop entirely new products, potentially hindering disruptive innovation that is urgently needed during Europe's twin transition.

A recent study by Demirer et al. provides a detailed insight into how the GDPR has changed firms' actual production processes.[34] In response to the GDPR, EU firms reduced data storage by 26% and data processing by 15% compared to similar US firms, becoming less "data intensive" and thus less ready to capitalise on AI innovations. By estimating a production function with data and computation as inputs, the study estimated that the GDPR effectively increased data costs by an average of 20% for affected firms. However, the impact varied significantly across industries and individual firms, highlighting that the concrete shape of the trade-off between data protection and data-based innovation might differ depending on relevant markets and individual company characteristics.

What is the overall picture? After several years, empirical evidence is beginning to emerge that the GDPR has had a profound impact on business operations in the EU, innovation trajectories, and competitive dynamics in the digital economy. While enhancing individual privacy protection, the regulation has imposed significant legal uncertainty and compliance costs, which are particularly challenging for SMEs and have accelerated trends of market consolidation and concentration in the hands of US Big Tech. Especially the observed shift towards incremental innovation and reduced data intensity in EU firms raises concerns about potential long-term impacts on technological progress and competitiveness. However, the GDPR has also spurred firms to re-evaluate and improve their data management practices, which may bring benefits in terms of data quality and consumer trust.

---

[31] Carl Benedikt Frey and Giorgio Presidente, 'Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally', *Economic Inquiry* 62, no. 3 (July 2024): 1074–89, https://doi.org/10.1111/ecin.13213.

[32] Christian Peukert et al., 'European Privacy Law and Global Markets for Data', CEPR Discussion Paper (London: Centre for Economic Policy Research, 2020), https://cepr.org/publications/dp14475.

[33] Knut Blind, Crispin Niebel, and Christian Rammer, 'The Impact of the EU General Data Protection Regulation on Product Innovation', *Industry and Innovation* 31, no. 3 (15 March 2024): 311–51, https://doi.org/10.1080/13662716.2023.2271858.

[34] Mert Demirer et al., 'Data, Privacy Laws and Firm Production: Evidence from the GDPR' (Cambridge, MA: National Bureau of Economic Research, February 2024), https://doi.org/10.3386/w32146.

3.2 Platform moderation: Regulation vs. freedom of expression, competitiveness & security

Since early 2024, the Digital Services Act (DSA) fully applies to services like search engines, online marketplaces, social media platforms, and video apps, which millions of people in the EU use daily. The DSA aims to create a safer digital environment for EU citizens and other persons. At the same time, it aims to safeguard the internal market by avoiding the fragmentation potentially deriving from diverging national regulations covering „diligence requirements for providers of intermediary services as regards the way they should tackle illegal content, online disinformation or other societal risks."[35] In practice, the DSA lays out novel obligations for digital firms, including social media behemoths like Facebook, Instagram, X, and TikTok. Although they are not considered liable for the content they publish, they have now to bear relevant costs related to transparency, content moderation, and compliance with key risk-related imperatives such as abstaining from deceptive practices and ensuring a high level of privacy, safety, and security of minors. They also face fines when they fail to comply with their obligations as laid out in the DSA.

Applying our trilemma to the case of the DSA, it becomes clear that, regardless of all the issues inevitably surrounding such type of pioneering regulation and its fast-evolving subject-matter, indeed at least three potential trade-offs are involved, depending on the standpoint one adopts: as further elaborated below, there is 1) a potential trade-off between the objective to create a safe and secure digital environment and individual rights and civil liberties, especially the freedom of speech; 2) a potential trade-off between the competitiveness of online platforms and the protection of individual rights and civil liberties; and 3) a potential trade-off between the competitiveness of online platforms and the objective to create a safe and secure digital environment.

A relevant issue hinges on the definition of „systemic risk" posed by "very large online platforms" (VLOP) and "very large online search engines" (VLOSE). This risk is primarily defined by the provider's reach, specifically when it exceeds an operational threshold of 45 million users, which is equivalent to 10% of the EU population. The DSA then specifically mentions four categories of risks: 1) risks associated with the dissemination of illegal content, such as child sexual abuse material or illegal hate speech; 2) the actual or foreseeable impact of the service on the exercise of fundamental rights, including the freedom of speech; 3) risks associated with negative effects on democratic processes, electoral processes, public security; 4) risks associated with the design, functioning or use, including through manipulation, of VLOP and VLOSE, which may have a negative impact on the protection of public health, minors and serious negative consequences to a person's physical and mental well-being, or on gender-based violence. In short, the EU legislator clearly specifies the justification, in terms of societal hazards, for regulating the activity of VLOP and VLOSE.

A key role in the implementation of the DSA is attributed to the so-called „trusted flaggers" that is non-governmental entities designed by national Digital Services Coordinators entrusted with detecting potentially illegal content and alert online platforms. According to the DSA, reports of suspected illegal content by trusted flaggers are to be treated with priority by online platforms. Indeed, the involvement

[35] REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065.

of non-governmental actors is an example of how the DSA is not simply strengthening state institutions vis-à-vis private actors, but also civil society and individuals vis-à-vis private actors.[36] Two recent legal articles offer contrasting perspectives on the role of trusted flaggers, highlighting the trade-offs between security, fundamental rights, and economic competitiveness. Ruschemeier takes a generally positive view of the trusted flagger system, as they contribute to "democracy hygiene" by helping to identify and report illegal content online.[37] She argues that the DSA creates clear guidelines for trusted flaggers and transparent procedures that can help balance the need for content moderation with the protection of free speech, as trusted flaggers do not make content removal decisions themselves. In contrast, Lindner argues that the trusted flagger system poses structural risks to freedom of expression.[38] He contends that trusted flaggers may lack the legal expertise to accurately determine what content is illegal, potentially leading to the removal of lawful speech. He raises concerns about the lack of transparency in the flagging process and the potential for a chilling effect on online discourse. These two contrasting legal views, each with its own merits, illustrate the delicate balance the DSA seeks to strike between security and fundamental rights (the first trade-off listed above): On the one hand, the trusted flagger system aims to improve the efficiency of content moderation and protect users from illegal content, in line with the EU's goals of digital security and sovereignty. On the other hand, there are legitimate concerns about potential overreach and the impact on freedom of expression, which is a core fundamental right.

Apart from legal arguments, it is important to notice that, due to a lack of financial incentives to apply to qualify as one, the number of trusted flaggers is currently very low.[39] In this context, it should also be recalled that the DSA provides for remedies for situations that could be qualified as "over-reaction", or "over-censorship", that is cases in which content published is removed after being mistakenly considered to be illegal by a provider. In what can be considered a balancing exercise, the DSA repeatedly references the need to protect the exercise of fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. In case of overreaction, users have three options: 1) internal complaint systems (Art. 20), which platforms must provide and which must be accessible, fair, and supervised by qualified staff, and which allow users to challenge content moderation decisions; 2) out-of-court dispute resolution (Art. 21), i.e. recourse to dispute resolution mechanisms through certified out-of-court bodies; or 3) judicial redress, i.e. recourse to national courts.[40]

The economic competitiveness aspect of our trilemma is likewise evident in this debate. While the DSA aims to create a safer digital environment that could foster innovation, increased regulatory burdens on platforms could hinder this, whether in balancing competitiveness with the regulation of individual rights, including freedom of speech, or in balancing competitiveness with content moderation as a way to pursue a safer digital environment (the second and third trade-offs mentioned above).[41] The costs associated with implementing robust content moderation systems and complying with the DSA may

[36] Martin Husovec, *Principles of the Digital Services Act.* Oxford: Oxford University Press (2024).

[37] Hannah Ruschemeier, 'Flagging Trusted Flaggers', 4 November 2024, https://doi.org/10.59704/6c2c9f4cc624f31a.

[38] Josef Franz Lindner, 'Trusted Flagger Als Gefahr Für Die Meinungsfreiheit', 8 November 2024, https://doi.org/10.59704/9460eb2652f47ea8.

[39] For a list of currently recognised trusted flaggers, see https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa

[40] See Aleksandra Kuczerawy, Remedying Overremoval: The Three-Tiered Approach of the DSA, https://verfassungsblog.de/remedying-overremoval/

[41] Indeed, considerations of "offline" security are also relevant here. For example, consider the case of UK far-right riots in August 2024, which were fuelled by fake news spread on X (formerly Twitter) (see https://www.politico.eu/article/united-kingdom-riots-elon-musk-x-twitter-fake-news-disinformation/).

be particularly challenging for smaller platforms or new entrants to the market. As the DSA is increasingly implemented, policymakers must remain vigilant in assessing whether the chosen approach effectively addresses these competing priorities without unduly compromising any aspect of the digital policy trilemma.

Interestingly, the same trade-offs between risk and harm mitigation on the one hand, and fundamental rights and freedom of expression on the other, will also be relevant in the AI Act, particularly in relation to the regulation of high-impact, general-purpose AI models. The AI Act, adopted in June 2024 and discussed in more detail below (see section 3.4), requires providers of these models to mitigate potential systemic risks, echoing similar obligations in the DSA. The definition of systemic risk in the AI Act is vague, encompassing "actual or reasonably foreseeable adverse effects on public health, safety, public security, fundamental rights or society as a whole". As civil society organisations have argued, this broad definition could lead to an overly cautious approach by AI providers, potentially stifling innovation and limiting the expressive capabilities of AI systems.[42] In addition, like the DSA, the AI Act's systemic risk provisions for general purpose AI models will be enforced by the European Commission, i.e. a political body. This arrangement raises concerns about the potential politicisation of enforcement decisions, as seen in the early implementation of the DSA under Commissioner Breton, who used politicised enforcement to blur the distinction between illegal information and (allowed) disinformation.

3.3 Cybersecurity guidelines: Security vs. economic interests

The EU's 5G Security Toolbox and, more generally, the EU's ambitious plans on cloud and computing infrastructure address cybersecurity risks. However, due to their focus on domestic manufacturing and data localisation, they may also strain economic relations with key technology providers and trade partners such as the US (for the cloud sector, think about AWS) and China (for electronic equipment, think about Huawei), impacting rapid and cost-effective technology adoption and, in case of a tit-for-tat trade war, the continent's traditional export sectors.

The EU Toolbox on 5G Cybersecurity, published in January 2020, aims to address cybersecurity risks associated with 5G networks. Essentially, it is a strategic framework adopted by the EU to address security risks in the rollout of 5G networks. It was developed by the Network and Information Systems (NIS) Cooperation Group based on the NIS Directive, which aims to enhance cybersecurity across the EU. The Toolbox identifies risks associated with 5G networks, particularly regarding reliance on high-risk suppliers like Huawei and ZTE, and proposes measures to mitigate these risks.

While the EU Toolbox is not legally binding for member states, it serves as a set of guidelines that states are encouraged to implement voluntarily. The measures rely on a risk-based approach, allowing individual member states to decide how to integrate them within their national cybersecurity frameworks. The lack of binding force means that implementation varies significantly across member states, contributing to uneven progress. While the EU's ability to enforce cybersecurity measures is constrained by the principle of national sovereignty in matters of security, the Commission has actively pushed member states to adopt its recommendations to ensure a coordinated approach, using political and financial incentives to encourage alignment with the Toolbox guidelines. Taking stock of the situation

[42] Calvet-Bademunt (2024), Safeguarding Freedom of Expression in the AI Era | TechPolicy.Press.

three years into the introduction of the Toolbox,[43] the Commission expressed in 2023 strong concern vis-à-vis "the risks posed by certain suppliers of mobile network communication equipment to the security of the Union, as reflected also by decisions taken by some Member States."[44]

By August 2024, only eleven EU member states had exercised (although to different extents) legal powers to restrict high-risk telecom suppliers like Huawei and ZTE from participating in 5G network infrastructure.[45] It should be noted that this does not necessarily translate into total bans – which in many cases would be technically and financially unfeasible. The German government, for instance, negotiated with mobile network operators an agreement to ensure the removal of Huawei and ZTE components from 5G core networks by the end of 2026. Additionally, critical management systems supplied by these two manufacturers in 5G access and transport networks are to be replaced with alternative technologies by the end of 2029.[46] Since 2019,[47] French authorities have the power to impose restrictions, prohibitions, or specific requirements on the supply, deployment, and operation of 5G equipment. This includes making it mandatory to obtain prior authorization from the Prime Minister for rolling out and operating sensitive equipment within 5G networks, as well as future telecommunications technologies (such as 6G).[48] Similarly, in Italy, as per new legislation introduced in 2022,[49] companies intending to acquire goods or services related to the design, implementation, maintenance, and management of broadband electronic communication services based on 5G technology must notify the Office of the Prime Minister with detailed information. This notification is required for the government to assess whether to exercise its veto power.

It should be noted that, echoing the concerns articulated by the Commission in 2023, in her recent confirmation hearing at the European Parliament Commissioner-designate for Tech Sovereignty, Security and Democracy Henna Virkkunen expressed dissatisfaction with the current state of implementation of the 5G Cybersecurity Toolbox, announcing a revision to the EU Cyber Security Act in 2025 as well as proposing a Digital Networks Act.[50]

Another illustrative example of potential trade-offs is the draft EU Certification Scheme for Cloud Services (CSCS). The CSCS and the EU Toolbox on 5G Cybersecurity serve as complementary components of the EU's broader cybersecurity strategy, but while the Toolbox focuses on securing 5G networks through risk mitigation measures, the EU CSCS should ensure that cloud services, which often support critical infrastructure like 5G, meet robust cybersecurity standards. Together, they address

---

[43] See: https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

[44] See: Communication by the Commission: : Implementation of the 5G cybersecurity Toolbox, https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox

[45] See: "Eleven EU countries took 5G security measures to ban Huawei, ZTE", https://www.euronews.com/next/2024/08/12/eleven-eu-countries-took-5g-security-measures-to-ban-huawei-zte

[46] See: „Greater security and technological sovereignty for the German 5G mobile network: The Federal Government concludes contracts with telecommunications companies", https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2024/07/5g-en.html

[47] Law 810/2019 of 1st August 2019 https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038864094

[48] Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity. https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity

[49] Law 108/2022 https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2022-08-05&atto.codiceRedazionale=22G00120&atto.articolo.numero=1&atto.articolo.sottoArticolo=1&atto.articolo.tipoArticolo=0

[50] See: „New EU tech chief to discuss 5G security measures with national governments", https://www.euronews.com/my-europe/2024/11/13/new-eu-tech-chief-to-discuss-5g-security-measures-with-national-governments.

interconnected risks in key technological areas, in line with the idea that the EU "should ensure that it has a competitive domestic industry that can meet the demand for 'sovereign cloud' solutions" contained in the so-called "Draghi Report" on the Future of European Competitiveness.[51]

Recently, the draft EU CSCS has been at the centre of a political battle over sovereignty requirements.[52] France but also representatives of EU digital SMEs are in favour of a stricter approach that would eventually exclude non-EU cloud services providers from operating at the highest security levels.[53] Other member states and industry actors fiercely opposed this idea, seeing it as a protectionist move. More generally, critics of the EU's plans argue that an approach that prioritises "digital sovereignty" – which aims to maintain European control over critical infrastructure and data, but also favours localisation policies, including in AI and quantum computing – would require excessive resources to keep up with global competitors, potentially diverting investment and human capital from other sectors.[54]

The debate surrounding the draft EU CSCS has exposed diverging preferences in EU member states with respect to the introduction of sovereignty requirements for service providers. Indeed, business organizations in countries such as Germany clearly expressed concern over the possibility that the introduction of such requirements would hamper the growth of European companies operating globally.[55] Clearly, this configures a trade-off between economic competitiveness and the pursuit of security and EU sovereignty. The new Commissioner for Tech Sovereignty, Security and Democracy will need to carefully consider this trade-off in developing the regulatory innovations in ICT infrastructure mentioned above.

3.4 AI regulation: Ethical standards vs. competitiveness

The EU's AI Act, which came into force on August 1, 2024, is a bold step towards establishing ethical standards for the development and use of AI, including in the realm of Large Language Models (LLMs). While this legislation aims to position the EU as a global leader in responsible AI, it also raises concerns about the potential impact on innovation and competitiveness. This trade-off between ethical considerations and economic competitiveness is not unique to AI regulation but is particularly relevant given the transformative potential of AI technologies. According to scholars from Bruegel, "it is unknown whether the Act will stimulate responsible AI use or smother innovation."[56]

LLMs, such as BERT, LLaMA and OpenAI's GPT series, have the potential to revolutionise the way we interact with information and communicate in the digital age. These models can significantly enhance our ability to retrieve and process information, potentially augmenting collective intelligence (CI) on a scale previously unimaginable. However, as a large group of researchers recently noted in *Nature*, this

---

[51] See: https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf.

[52] See: https://www.euronews.com/next/2024/06/18/decision-on-cloud-certification-scheme-delayed-to-mid-july.

[53] See: https://www.digitalsme.eu/changes-to-the-eu-cloud-services-cybersecurity-certification-scheme-put-eu-citizens-data-at-risk-a-call-for-digital-sovereignty/

[54] See, e.g.: Matthias Bauer, Fredrik Erixon, and Dyuti Pandya, 'The EU's Trillion Dollar Gap in ICT and Cloud Computing Capacities: The Case for a New Approach to Cloud Policy', ECIPE Occasional Paper (Brussels: European Centre for International Political Economy (ECIPE), 2024), https://hdl.handle.net/10419/299187.

[55] See: Julia Rone, '"The Sovereign Cloud" in Europe: Diverging Nation State Preferences and Disputed Institutional Competences in the Context of Limited Technological Capabilities', *Journal of European Public Policy* 31, no. 8 (2 August 2024): 2343–69, https://doi.org/10.1080/13501763.2024.2348618.

[56] See: The European Union AI Act: premature or precocious regulation?.

power comes with inherent risks and trade-offs.[57] The very diversity and individual competence that contribute to CI in human systems may be compromised if LLMs homogenise information sources or reduce the need for individual critical thinking. Furthermore, the aggregation mechanisms that are critical for CI need to be carefully considered when integrating LLMs into collective decision-making processes. The potential for LLMs to both support and possibly undermine CI highlights the delicate balance that must be struck in their development and regulation.

The potential impact of AI regulation on innovation and competitiveness has been the subject of considerable debate and research.[58] A comprehensive study conducted by the Centre for European Policy Studies (CEPS) in 2020 estimated that compliance costs for companies subject to the AI Act could be between 1% and 4% of AI-related revenues. It is important to note, however, that these costs would primarily apply to high-risk AI systems, which are estimated to represent only 5-15% of all AI systems. The study notes that many companies already comply with some of the proposed requirements as part of their standard business practices, potentially reducing the additional compliance burden. Still, the costs associated with implementing quality management systems for high-risk AI products could be significant for SMEs, potentially ranging from €193,000 to €330,000 for initial setup, with an additional €71,400 for annual maintenance. It is important to approach cost estimates with caution and to consider the broader context. The CEPS researchers themselves have emphasised that the results of their study have been misinterpreted by some, leading to exaggerated cost projections.

As the EU AI Act's approach targets specific high-risk applications rather than entire sectors, it is also likely that the trade-off between regulation and innovation may vary across industries.[59] In the healthcare sector, the interplay between the AI Act and existing regulations such as the Medical Devices Regulation (MDR) and the In Vitro Diagnostic Medical Devices Regulation (IVDR) may increase the compliance burden for manufacturers. However, it also has the potential to increase patient safety and trust in AI-powered medical solutions. Similarly, in financial services, the AI Act's focus on high-risk applications could lead to increased oversight of AI-powered credit scoring, pricing models, and risk assessments. This increased scrutiny is intended to protect consumers and maintain market stability, but it may also slow the adoption of innovative AI-powered financial products. Finally, in the automotive industry, the AI Act could provide much-needed clarity on the regulatory framework for autonomous vehicles. While this could simplify some aspects of development and deployment, it also introduces new requirements around safety standards.

In light of these trade-offs, looking at the lessons learned from past regulatory efforts might provide insights for implementing the AI Act. Aghion, Bergeaud, and Van Reenen examined the impact of (labour) regulations on innovation in France.[60] They found that firms just below the regulatory threshold of 50 employees showed a sharp reduction in innovation, particularly in response to market opportunities. Overall, the researchers estimated that regulation reduced aggregate innovation by about 5.4%, equivalent to a 2.2% loss in consumption-equivalent welfare. Importantly, the study found that most of this loss in innovation was due to a reduction in the intensity of innovation per firm, rather than simply a misallocation of resources to smaller firms or reduced market entry. This suggests that the impact of regulation on innovation is more complex than simply changing market structure. However,

---

[57] Jason W. Burton et al., 'How Large Language Models Can Reshape Collective Intelligence', *Nature Human Behaviour* 8, no. 9 (20 September 2024): 1643–55, https://doi.org/10.1038/s41562-024-01959-9.

[58] For this summary, see: Clarifying the costs for the EU's AI Act – CEPS.

[59] See: European AI Act: Opportunities and challenges | Roland Berger.

[60] See: Blind, Niebel, and Rammer, 'The Impact of the EU General Data Protection Regulation on Product Innovation'.

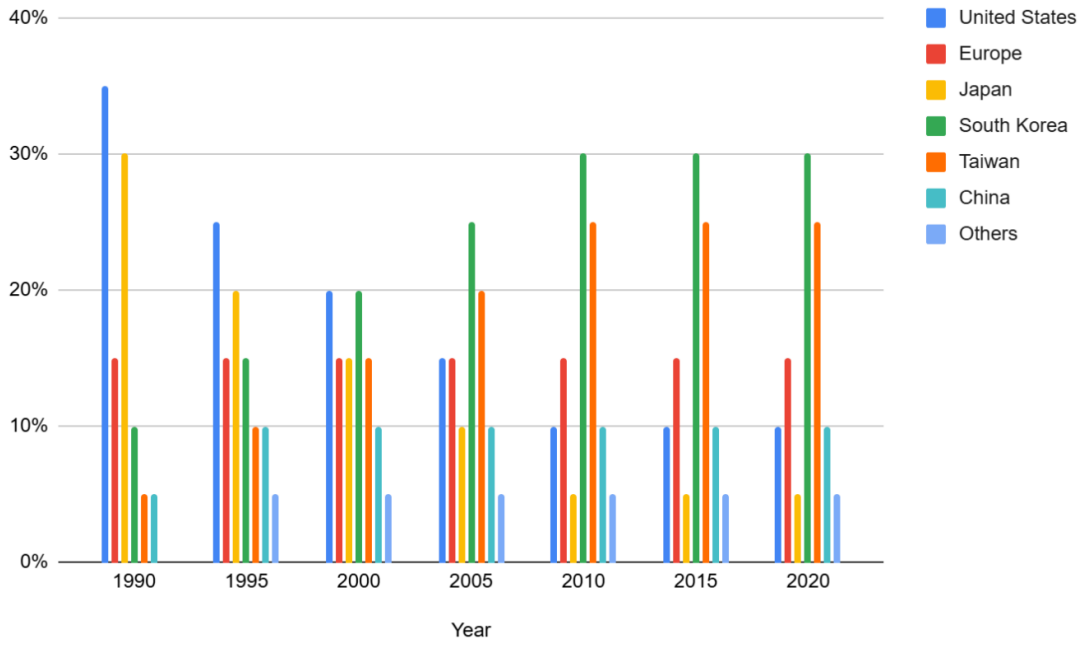
the research also uncovered an interesting nuance: while regulation appeared to reduce incremental innovation, it seemed to encourage more radical, labour-saving breakthroughs. Firms operating under stricter regulation tended to enact more ambitious innovation projects when they did innovate.

These findings might provide some insights for the implementation of the AI Act. Policymakers should carefully design and repeatedly re-evaluate regulatory thresholds to avoid stifling innovation incentives, especially for firms close to these boundaries. Establishing mechanisms for ongoing assessment of the AI Act's impact on both the intensity and direction of innovation will be crucial for refining the regulatory framework over time. Given the disproportionate impact on smaller firms, targeted support or exemptions for SMEs in the AI sector could help maintain a diverse and innovative ecosystem. Finally, as regulation can affect global competitiveness, fostering international cooperation on AI governance could create a more level playing field while promoting responsible AI standards globally, a point to which we return below (section 4).

3.5 Computing infrastructure: Strategic autonomy vs. global cooperation

The global struggle for control of microchip technology has become a critical geopolitical battleground with far-reaching implications for economic power, military capabilities, and technological progress.[61] This competition, once primarily between the US and China, has now expanded to include Europe as a major player. The EU's response to this challenge is twofold, addressing both the hardware and software aspects of computing infrastructure. On the one hand, the EU Chips Act aims to strengthen Europe's semiconductor industry and reduce dependence on foreign suppliers. On the other, the recent EU AI Factories initiative aims to leverage Europe's existing strengths in high-performance computing to accelerate the development of AI. We will discuss both angles in turn.

Fig. 2: Semiconductor manufacturing capacity by region, 1990-2020



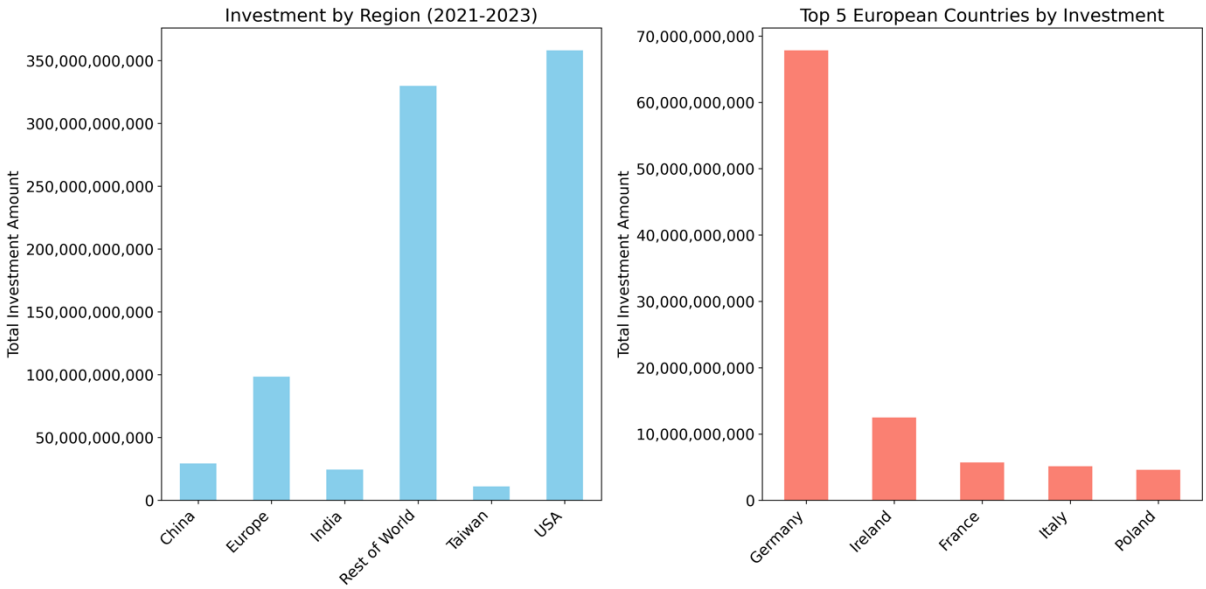
Source: BofA Global Research. Taken from: Artisan Partners Growth Team, The Semiconductor Decade.

[61] Chris Miller, *Chip War: The Fight for the World's Most Critical Technology* (London: Simon & Schuster Ltd, 2023).

Over the past two decades, the global semiconductor industry has become increasingly reliant on a handful of manufacturers in East Asia, particularly for leading-edge chips (Figure 2). The more sophisticated "front-end" chip production processes are concentrated in the US, Taiwan, and South Korea, increasingly in China, and to a smaller (and decreasing) extent in Europe, while Southeast Asia specializes in back-end semiconductor manufacturing.[62] Taiwan Semiconductor Manufacturing Company (TSMC) and Samsung Electronics in South Korea have emerged as the dominant players in producing the most advanced chips, with TSMC alone accounting for over 90% of the global production of chips at the 5-nanometer node and below. This concentration has been driven by the enormous capital investments required to maintain technological leadership and the benefits of economies of scale.

While other countries and regions have long invested in semiconductor industry development, the introduction of the European Chips Act marks a new trend, as the EU seeks to achieve strategic autonomy in this industry. The reasons why this is happening now are manifold. The pandemic exposed the supply chain dependency of the EU and its vulnerability in the face of unforeseen geopolitical events. Semiconductors supply security suddenly came to the fore as a key priority for the EU, especially as a result of shortages experienced in the automotive industry. In general, chips are crucial to the development of green technologies considering that the decarbonization of the economy has become a policy priority. This underscores the need for a "diversified geography of production."[63] In other words, the European Chips Act signals a shift from the "just-in-time" model typical of an optimistic view of economic globalization to a more cautious "just-in-case" approach to supply chain management that has emerged in response to the pandemic and recent geopolitical crises.

Fig. 3: Investment in chips, 2021-2023



Own illustration and data analysis. Data scraped from: SemiconductorEngineering website.

[62] As opposed to „front-end" semiconductor manufacturing, which consists in the creation of the semiconductor structures resulting in the production of a silicon wafer, the „back-end" phase consists in cutting the wafer, assembling, packaging and testing the final product. See: https://www.rabobank.com/knowledge/d011371771-mapping-global-supply-chains-the-case-of-semiconductors.

[63] See: Lindsay Whitfield et al., 'European Chips Act and the Global Race in Semiconductor Industrial Policy: Business in Development; E7.(Denmark: Centre for Business and Development Studies, 24 June 2024).

To consider the scale and effectiveness of Europe's re-orientation, we examined data compiled from two comprehensive online reports published by Semiconductor Engineering, detailing new plant and "fab" investments announced between 2021 and 2023.[64] The data has been manually aggregated from company announcements and press releases, providing a snapshot of the industry's expansion plans over this period. To ensure consistency in our analysis, all investments were converted into US dollars using approximate exchange rates at the time of announcement. Where a range of investments was provided, we used the upper estimate to capture the full potential of the project. For some investments, specific financial details were not disclosed. Our dataset covers a three-year period from 2021 to 2023, capturing the initial wave of investment announcements following the global chip shortage and subsequent policy responses. However, the semiconductor industry is cyclical, and some announced investments may have been modified or cancelled since their initial announcement.[65] Investment types have been broken down to reflect nuanced categories (e.g. "advanced packaging") that often co-occur within the same entries, and regional distinctions have been applied to compare spending across the US, Europe, China, India, Taiwan and other regions.

The (blue) left-hand panel in Figure 3 shows the distribution of semiconductor industry investment across the world's major regions. The US is clearly the leading region, with total investments exceeding $350 billion, in line with the US CHIPS Act. The "Rest of the World" category, which includes various markets such as Japan, South Korea, Vietnam, Malaysia, and Singapore, also shows a notable level of investment in the magnitude of around $300 billion. Following its own EU Chips Act, Europe is aiming to catch up, with cumulative investments of roughly $100 billion. Meanwhile, investment levels in regions such as Taiwan, India, and China are comparatively modest. This distribution essentially reflects the recent push by leading economies to strengthen their semiconductor sectors amid global supply chain concerns, positioning the US as a dominant hub.

The (red) right-hand panel of Figure 3 illustrates a significant disparity in the distribution of semiconductor investment *within* Europe, with Germany alone attracting the overwhelming majority of funding, totalling around $70 billion. In stark contrast, other EU countries such as Ireland, France, Italy, and Poland receive much smaller shares. This distribution points to a certain distortion in the EU's single market. Such an imbalance can, later on, exacerbate technological dependencies within the EU and reduce the resilience of the semiconductor supply chain across the region. In other words, this type of industrial policy could have detrimental effects on intra-EU economic convergence.[66]

We also analyse the data qualitatively to gain insight into the specific areas of semiconductor technology where significant investment has been concentrated. Significant investment has been focused on foundry chip manufacturing, with $228 billion allocated to this category, underscoring the industry's emphasis on expanding core manufacturing capabilities. In addition, $100 billion was invested in the upgrade of high-NA EUV lithography tools at Intel's Gordon Moore Park campus in the US, a next-generation lithography technology critical to chip size reduction. In terms of advanced manufacturing, there has been significant investment in 3nm process technology, particularly in regions such as the

[64] See: https://semiengineering.com/money-pours-into-new-fabs-and-facilities/ (investments announced in 2023 and late 2022) and https://semiengineering.com/where-all-the-semiconductor-investments-are-going/ (investments announced in 2021 and 2022).

[65] A notable example is Intel's planned investment in Germany, which has been revised since it was first announced.

[66] On this point, see: Angela Wigger, 'The New EU Industrial Policy and Deepening Structural Asymmetries: Smart Specialisation Not So Smart', *JCMS: Journal of Common Market Studies* 61, no. 1 (January 2023): 20–37, https://doi.org/10.1111/jcms.13366.

US and Taiwan, which are likely to seek to maintain technological leadership through advanced semiconductor manufacturing. In contrast, we observe a broader focus on various areas of semiconductor infrastructure and capacity expansion in other regions of the world, including in Europe. Investments in 300mm wafers, new fabs, and general semiconductor manufacturing infrastructure suggest a commitment to building foundational capacity rather than focusing exclusively on leading-edge technology nodes. The presence of $20 billion in investments in areas such as quantum computing, AI, and hybrid cloud further indicates a diversified investment strategy. In addition, significant investments in assembly and test units and a display fab unit suggest a focus on downstream production capabilities that support the broader semiconductor supply chain. Overall, the US and Taiwan appear to be focusing heavily on high-tech innovation and cutting-edge manufacturing processes, while Europe and other regions are prioritising the expansion of production capacity and infrastructure.

Complementing the manufacturing-focused Chips Act, the EU's new "AI Factories" initiative aims to increase investment in the hardware and software infrastructure critical to generative AI development. Launched in early 2024, this €2 billion programme aims to create a network of AI-optimised supercomputers accessible to researchers, startups, and industry across Europe.[67] By leveraging the existing capabilities of the European High-Performance Computing Joint Undertaking (EuroHPC JU), the initiative aims to democratise access to the computational resources needed to develop large-scale AI applications.

However, the initiative, while ambitious, seems to suffer from similar conceptual challenges as the European chip subsidies described above. Both initiatives lack a truly centralised industrial policy, which is essential to avoid market distortions and ensure an efficient allocation of resources. The AI factories plan, like its semiconductor counterpart, risks fragmentation by attempting to spread resources across several Member States to satisfy political demands rather than focusing on the most efficient solutions. This approach could lead to a dilution of funding and a lack of the critical mass needed to compete on a global scale. As Hoos points out, the EU's planned investment in each AI factory is in the "wrong order of magnitude", with only tens of millions of euros allocated per facility.[68] This piecemeal approach contrasts sharply with the massive investments being made by US firms like OpenAI and Microsoft, who are planning a $100 billion data centre by 2028.

3.6 Competition policy: Consumer welfare vs. broader public interests

Throughout Europe, the field of competition law has lately been seen as a highly technical discipline, focused primarily on economic analysis and the prevention of non-optimal pricing by large companies.[69] During the past decades, particularly during the "More Economic Approach" era, competition policy was characterised by its reliance on complex econometric models and quantitative assessments.[70] While rigorous, this approach often overlooked broader societal implications and normative

[67] See: https://digital-strategy.ec.europa.eu/en/policies/ai-factories.

[68] See: https://www.euractiv.de/section/innovation/news/ki-computing-eu-kaempft-mit-rueckstand-und-investitionsluecke/.

[69] Oles Andriychuk, *The Normative Foundations of European Competition Law: Assessings the Goals of Antitrust through the Lens of Legal Philosophy* (Cheltenham, UK: Edward Elgar Publishing, 2017).

[70] André Schmidt and Michael Wohlgemuth, 'Das Wettbewerbskonzept der EU aus Sicht der Wirtschaftswissenschaften: Wie ökonomisch ist der „more economic approach"?', in *Dimensionen des Wettbewerbs: europäische Integration zwischen Eigendynamik und politischer Gestaltung*, ed. Hermann-Josef Blanke, Arno Scherzberg, and Gerhard Wegner, Neue Staatswissenschaften 11 (Tübingen: Mohr Siebeck, 2010), 51–80.

values beyond pure economic efficiency. The narrow focus on technical analysis served to insulate competition law from external considerations, creating a somewhat insular field of expertise that ignores potential trade-offs. This approach differs from that of strategic rivals such as China, which uses antitrust to promote domestic firms and as an instrument of trade and foreign policy.[71]

However, recent years have seen a cautious shift in the EU's competition policy paradigm. The unprecedented scale and scope of digital platforms has forced policymakers and academics to recognise that the power wielded by tech giants not only affects market competition, but also has profound implications for privacy, democracy, and social cohesion.[72] As a result, there is a growing recognition that competition policy cannot operate in isolation from these broader societal concerns. The pandemic has further underlined the need for a more holistic approach to competition policy. As the Covid crisis exposed vulnerabilities in global supply chains and highlighted the risks associated with monopolies and single points of failure in critical industries, a debate emerged on the role of competition law in promoting economic resilience and safeguarding essential services in times of crisis. Another novel area of debate is the concept of "green antitrust", which seeks to integrate sustainability considerations into EU competition analysis.[73] Proponents argue that competition policy should evolve to support sustainable business practices and cooperative efforts to reduce environmental damage, even if such actions may appear to restrict competition in the short term.

The potential for a Trump 2.0 presidency – which now has materialised – has further intensified these debates. The early threat by J.D. Vance to withdraw US support for NATO if the EU continues to investigate Elon Musk's X platform is an example of the growing intersection between platform regulation and geopolitical considerations.[74] Should the EU maintain the integrity and independence of competition enforcement in the face of external political pressure and national security concerns? During her parliamentary hearing, incoming EU Tech Commissioner Henna Virkkunen avoided addressing Musk's role in spreading misinformation on X – marking a stark contrast to her predecessor, Věra Jourová, who had called Musk a "promoter of evil." [75] Instead, Virkkunen highlighted the dual challenge she faces: ensuring European security, which relies heavily on US cooperation, while advancing European tech sovereignty, often at odds with American tech giants.

How to handle these new types of non-economic trade-offs from a competition policy perspective? Martijn Snoep, Chairman of the Dutch Authority for Consumers and Markets, recently noted that while competition authorities are well equipped to analyse market dynamics and propose measures to enhance competition, they are not always best placed to take the final decisions when other critical public interests are at stake.[76] As Snoep points out, "what may be good for competition may be bad for, say, national security or privacy", so he proposed an additional guardrail that would give a minister the power to overrule, in whole or in part, any measure a competition authority proposes to impose if it conflicts with broader public interests. By introducing ministerial oversight, this system would allow

---

71 Zhang, *Chinese Antitrust Exceptionalism*.

72 Patrick Barwise and Leo Watkins, 'The Evolution of Digital Dominance: How and Why We Got to GAFA', in *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, ed. Martin Moore and Damian Tambini (Oxford: Oxford University Press, 2018), 21–49, https://doi.org/10.35065/PUB.00000914.

73 Maarten Pieter Schinkel and Leonard Treuren, 'Green Antitrust: Friendly Fire in the Fight against Climate Change', *SSRN Electronic Journal*, 2020, https://doi.org/10.2139/ssrn.3749147.

74 See: https://www.independent.co.uk/news/world/americas/us-politics/jd-vance-elon-musk-x-twitter-donald-trump-b2614525.html.

75 Politico (2024), 5 things to know about EU tech security chief Henna Virkkunen's hearing – POLITICO.

76 See: https://www.acm.nl/en/publications/blog-martijn-snoep-updating-competition-enforcement.

for a more comprehensive assessment of proposed competition measures against a wider range of societal concerns. This ministerial override power would be similar to existing mechanisms in Germany, where ministers for economic affairs can override competition authority decisions in merger cases on general public interest grounds. From an ordoliberal perspective, however, the implementation of this approach would require careful design to ensure transparency and to avoid undue political interference in competition matters. Clear criteria for ministerial intervention and public justification for any overrides would be essential to maintain the integrity of the competition enforcement process.

4 External dimension: Addressing trade-offs through partnerships

While it is sometimes underestimated, the external dimension of EU digital policy offers several opportunities to address some of the trade-offs identified in the previous sections. While international engagement is often perceived as a source of potential risks, a strategic approach to partnerships and cooperation could actually serve as a solution to many of the EU's digital challenges. This perspective may seem counterintuitive given the prevailing narrative of geopolitical struggles, cultural clashes, digital sovereignty, and self-reliance, but it offers a promising way to address complex policy dilemmas. By fostering cooperation with international partners, we argue below, the EU can actually enhance its technological capabilities and strengthen its security measures, while mitigating some of the internal trade-offs that have emerged in its digital policy landscape. This is similar to the arguments made by Renda, who recently argued that "only by embedding rules and values in 'code' and preserving openness towards the rest of the world will the EU manage to achieve its desired goals".[77]

The European Union (EU) has taken significant strides to establish itself as a global leader in digital diplomacy.[78] This transformation was first marked by the digital single market initiative launched in 2015, which evolved from a largely domestic-focused project into one with extensive international ambitions, as per the "2030 Digital Compass" launched in 2021.[79] The EU's approach to digital diplomacy has incorporated a multi-layered framework that includes digital regulations, international collaborations, development cooperation, and policy alignment with member states. In the context of the EU institutional framework, several key Directorate-Generals (DGs) within the European Commission contribute to shaping EU digital diplomacy. DG Connect (Communications Networks, Content and Technology) has evolved from a research-focused branch into a policy-driven entity, working on digital regulation, international digital partnerships, and major research initiatives like the 5G PPP. DG Grow (Internal Market, Industry, Entrepreneurship and SMEs) drives initiatives for the digital transformation and decarbonization of European industry and SMEs, supporting the goal of making the EU a greener, more digital, and resilient economy. DG Intpa (International Partnerships) emphasizes the integration of digital initiatives within development policy, driven by the increasing relevance of digital technology across areas such as agriculture, water resources, and human rights in partner countries. DG Trade has

[77] Andrea Renda, 'Making the Digital Economy "Fit for Europe"', *European Law Journal* 26, no. 5–6 (November 2020): 202, https://doi.org/10.1111/eulj.12388.

[78] Here, *digital diplomacy* refers to a broader concept, highlighting diplomatic efforts concentrated on strategically critical policy areas such as cybersecurity, data protection, e-commerce, internet governance, and AI governance. These topics influence nearly every policy domain relevant to the EU, from geopolitics and development to human rights and security. See: Cecilia Emma Sottilotta, 'A "Battle for Hearts and Minds"? EU Digital Diplomacy toward the Global South', *Global Policy*, 22 August 2024, 1758-5899.13423, https://doi.org/10.1111/1758-5899.13423.

[79] See: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2030 Digital Compass: the European way for the Digital Decade, COM/2021/118 final.

intensified its focus on digital trade, particularly in negotiations on data flows, while DG Just (Justice and Consumers) collaborates to ensure data privacy and rights are maintained within these exchanges. DG Research and Innovation funds critical digital infrastructure projects that support EU digital diplomacy efforts, such as the geo-strategically important Bella cable linking Europe and Latin America, and Medusa, spanning the Mediterranean. Last but not least, the European External Action Service (EEAS) plays a key role in coordinating EU digital diplomacy efforts. Following the Council Conclusions on EU Digital Diplomacy in 2022 and 2023, the EU laid out priority actions for a more strategic and cohesive digital policy, emphasizing a "Team Europe" approach for coordinated global engagement on digital issues.[80] These actions focus on strengthening multilateral partnerships, addressing digital divides, and advancing leadership in global digital standards, especially in emerging technologies. More recently, the Foreign Affairs Council's review in July 2024 highlighted the strategic importance of digital issues in EU foreign policy and the need for unified action to support democracy, the economy, and society.

How could cooperation and partnerships help address the specific trade-offs identified above?

1. To begin with, the EU can use international partnerships to balance its high data protection standards with the need to foster a competitive business environment. The EU's mutual adequacy decisions for the transfer of personal data with Japan (2019) and South Korea (2021), respectively, are examples of successful cooperation, facilitating the free flow of personal data while maintaining strong privacy protections. Looking back, countries that received EU adequacy saw an increase in digital trade of between 6% and 14 %, representing a reduction in trade costs of up to 9%.[81] However, civil liberties organisations have argued that the Commission's positive assessment of the EU-US Data Protection Framework (DPF) downplays significant concerns about state and commercial surveillance, effectively perpetuating the mass surveillance practices revealed by Edward Snowden over a decade ago.[82] Furthermore, the second Trump presidency further complicates the situation. During his first term, President Trump's administration took a confrontational stance towards the EU's privacy frameworks, arguing that they hindered US businesses and posed risks to national security.[83] His administration's efforts to strip non-US citizens of privacy protections under the Privacy Act exemplified this approach, leading to concerns that the DPF could be undermined or rendered ineffective if similar measures were reinstated. As the EU seeks to redefine its relationship with the US, the question is whether Europeans are willing and able to compromise on data protection in the face of geopolitical pressures.

Beyond DPFs, in December 2020 the EU launched the D4D Hub (Digital for Development Hub), an initiative aiming to promote inclusive and sustainable digital transformation globally. It is part of the EU's Global Gateway strategy and focuses on fostering digital partnerships with countries in Africa, Latin America, Asia, and the Pacific.[84] The D4D Hub aims to harness the EU's technological expertise and values, emphasizing connectivity, cybersecurity, and capacity-building, while also encouraging private

[80] See: EU digital diplomacy: Council agrees a more concerted European approach to the challenges posed by new digital technologies - Consilium; and Digital diplomacy: Council sets out priority actions for stronger EU action in global digital affairs - Consilium.

[81] Martina Francesca Ferracane et al., 'Digital Trade, Data Protection and EU Adequacy Decisions', Working Paper, EUI RSC (Florence: European University Institute, 2023), https://hdl.handle.net/1814/75629.

[82] Krempl (2024), Vorwürfe zum EU-US-Datenaustausch: Kommission spielt Massenüberwachung herunter | heise online.

[83] Vinocur (2020), Why Trump's administration is going after Europe's privacy rules – POLITICO.

[84] The EU Global Gateway Initiative, launched in December 2021, is the European Union's flagship strategy to mobilise investments for global infrastructure development. It aims to strengthen economic, social, and environmental resilience worldwide by promoting sustainable, high-quality, and values-driven projects in areas such as digital connectivity, energy, transport, health, and education. The initiative is widely seen as the EU's response to China's Belt and Road Initiative (BRI) and the US-led Partnership for Global Infrastructure and Investment (PGII).

sector investments. Examples of its activities include the EU-AU Data Governance Initiative, supporting African Union (AU) member states in developing data protection laws and digital governance frameworks aligned with international standards, the EU-LAC Digital Alliance, promoting policy exchange and cooperation on issues like digital governance, emerging technologies, and cybersecurity, or the India-EU ICT Standards Partnership, promoting the adoption of EU-aligned standards for 5G, IoT, and AI in India, ensuring interoperability and secure networks. Building on these partnerships, the EU could further refine the GDPR by incorporating more flexible mechanisms that support data-driven innovation. For example, the introduction of regulatory sandboxes or streamlined processes for international data transfers could address businesses' concerns about the GDPR's impact on competitiveness without compromising individuals' privacy rights.

2. When it comes to regulating online content and freedom of expression, international cooperation offers valuable insights into alternative approaches, including in the context of multi-stakeholder groups such as the UN Internet Governance Forum. As described above, the EU's DSA aims to create a safer digital space by holding online platforms accountable for the content they host. Engaging with democratic partners such as New Zealand, which spearheaded the so-called "Christchurch Call" to eliminate terrorist and violent extremist content online, or South Korea, known for its proactive measures against online hate speech and misinformation, could inform the large-scale implementation of the DSA over the coming years, ensuring that it effectively balances the protection of users with the preservation of freedom of expression. A key area where the EU could draw inspiration is Australia's push for technological age verification on social media platforms. The DSA has faced challenges in effectively implementing age verification measures, and Australia's approach might offer solutions.[85]

3. In the area of cybersecurity and economic incentives, partnerships with other technologically advanced nations could strengthen the EU's capabilities while sharing the economic burden. The EU's Cybersecurity Strategy for the Digital Decade emphasises the importance of international cooperation to improve cyber resilience. Joint research and development initiatives with countries such as Israel, known for its robust cybersecurity sector, or Singapore, a leader in cybersecurity innovation, as well as Japan and South Korea could strengthen the EU's technological resilience. Recent research by Wolf supports this approach, highlighting the crucial role of cross-border knowledge sharing in fostering innovation, especially in critical technology areas.[86] His analysis of global patent data shows that the EU lacks comparative technological advantages in several critical areas, including AI and connectivity. This underlines the need for international partnerships to boost the EU's technological capabilities. Importantly, Wolf finds that EU patents resulting from research collaborations with third countries received significantly more citations than those with purely domestic inventors, and thus recommends that the EU develop a dedicated technology cooperation strategy. Such partnerships would facilitate knowledge transfer, foster innovation, and potentially lead to new economic opportunities in the EU's digital economy. As mentioned earlier, the EU has recently started to experiment with some regulatory mechanisms that could be helpful in this regard: Regulatory sandboxes, as highlighted in the New European Innovation Agenda, provide a controlled real-world environment to test innovations with temporary adjustments to regulations.[87] These could facilitate collaborative experimentation between the

[85] See: https://www.rte.ie/news/business/2024/1126/1483039-meta-regulation-on-age-verification/.

[86] André Wolf, 'Forschungskooperationen Bei Kritischen Technologien: Europas Strategischer Balanceakt', *Zeitschrift Für Wirtschaftspolitik*, 13 November 2024, https://doi.org/10.1515/zfwp-2024-2021.

[87] European Commission, 'Regulatory Learning in the EU: Guidance on Regulatory Sandboxes, Testbeds, and Living Labs in the EU, with a Focus Section on Energy', Commission Staff Working Document (Brussels: European Commission, August

EU and its international partners, ensuring the development of safe, scalable, and effective cybersecurity technologies. Similarly, testbeds focused on technological advancements could offer a space for pioneering cybersecurity tools and systems developed in partnership with global leaders to be evaluated without regulatory constraints. Finally, so-called living labs, with their emphasis on co-creation and user involvement, could enable firms from EU member states and partner nations to collaboratively design, test, and refine cybersecurity measures that align with societal needs.

4. The development of ethical standards for AI is another area where international cooperation should be pursued, to avoid the loopholes characterising the current approach to "AI sovereignty" that, according to Mugge, pits the EU against the "Rest".[88] Rather than pursuing AI risk reduction in isolation, the EU should focus on multilateral efforts such as the Global Partnership on Artificial Intelligence (GPAI), which includes important members such as Canada, Japan, Australia, and the US. In line with this perspective, Germany's Federal Minister for Digital Affairs and Transport, Volker Wissing, recently emphasised the importance of global alliances in digital policy. In an interconnected world where the conditions for a free internet cannot be set unilaterally, he calls for greater engagement in international fora such as the G7, the OECD, and the Internet Governance Forum (IGF) to help shape global standards in line with shared values.[89] By engaging with diverse stakeholders, including STEM professionals, policymakers, and underrepresented communities, initiatives like those led by IEEE and UNESCO have made significant progress in establishing ethical frameworks for AI.[90] To address challenges in implementation and adoption, a more structured integration of technical knowledge into comprehensive AI governance agendas is needed.

5. When it comes to the trade-off between strategic autonomy and global cooperation in large-scale computing infrastructure, the EU can benefit from targeted partnerships, but also needs to develop its domestic capabilities to mitigate the risks associated with over-reliance on external systems such as SpaceX's Starlink. As highlighted in the previous section, the European semiconductor sector faces a risk of fragmentation due to an internal subsidy race driven by disparate state aid policies among Member States. To address this challenge, the EU must first phase out temporary frameworks like those introduced for the pandemic and energy crisis by the end of 2025, focusing instead on permanent instruments such as the GBER and IPCEIs to align national initiatives with a pan-European strategy.[91] Strengthening the IPCEI instrument is critical, with the Commission playing a greater role in ensuring projects are selected based on strategic merit rather than the fiscal capacity of individual Member States. Once these internal rules of the game are set, the EU could work with trusted partners to complement its resources, such as Japan, which is developing next-generation supercomputers. However, there is no way around developing its own capabilities through initiatives such as the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²) programme and the EuroHPC JU. As part of the subsidies and geopolitical rivalries discussed above, the global semiconductor landscape is

2023), https://research-and-innovation.ec.europa.eu/document/download/fc6f35cd-a8d6-4770-aefe-c09ca85cff8c_en?filename=swd_2023_277_f1.pdf.

88 Daniel Mügge, 'EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?', *Journal of European Public Policy*, 28 February 2024, 1–26, https://doi.org/10.1080/13501763.2024.2318475.

89 Wissing (2024), Wir brauchen mehr globale Allianzen - Tagesspiegel Background.

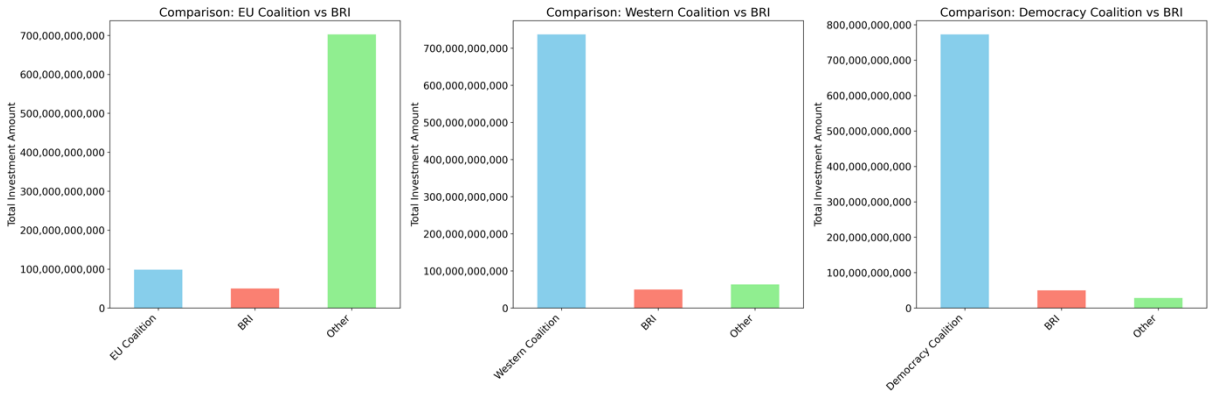
90 See: Mariazel Maqueda López et al., 'Science and Technology: A Framework for Peace', *Communications Engineering* 3, no. 1 (5 November 2024): 4, https://doi.org/10.1038/s44172-024-00310-4.

91 Donato Di Carlo, Andreas Eisl, and Diane Zurstrassen, 'Together We Trade, Divided We Aid: Mapping the Flexibilization of the EU State Aid Regime across GBER, IPCEIs and Temporary Frameworks', Policy Paper (Jacques Delors Institute, November 2024), https://institutdelors.eu/en/publications/together-we-trade-divided-we-aid/.

undergoing a seismic shift, with the US, EU, and other regions enacting ambitious legislation to strengthen domestic chip production and reduce dependence on foreign suppliers. TSMC's apparently successful expansion into Arizona,[92] backed by up to $6.6 billion in US government funding, is an example of how international partnerships can help address trade-offs in technological sovereignty. By bringing leading-edge 3nm and 2nm chip production to US soil, this collaboration enhances US economic competitiveness and national security while providing TSMC with a stable manufacturing base that is less exposed to potential conflict in the Taiwan Strait. Unlike the US, the EU lacks a dominant chipmaker like Intel and is therefore even more reliant on attracting foreign investment. However, achieving the goals of the EU Chips Act will require not only substantial funding, but also close cooperation with global industry leaders. By fostering partnerships with companies like TSMC and Intel, while strengthening ties with democratic allies like Japan and South Korea, the EU can leverage external expertise to build a more resilient and competitive semiconductor ecosystem.

The trade-off between strategic autonomy and global cooperation in large-scale computing infrastructure is a critical challenge for the EU in the context of competing global initiatives such as China's Belt and Road Initiative (BRI). The BRI is a global development strategy launched by China to improve international trade and infrastructure connectivity by investing in a global network of trade routes, ports and digital infrastructure across Asia, Africa, Europe, and beyond. To analyse the scale of the challenge, we have grouped countries into three coalitions – the EU Coalition, the Western Coalition and the Democracy Coalition. The EU Coalition consists of all EU member states and closely associated European countries. The Western Coalition expands this grouping to include traditional Western allies such as the US, Canada, Australia, Japan, South Korea and Israel, i.e. a broader alliance of liberal democracies. Finally, the formal Democracy Coalition includes not only Western nations but also democracies from other regions, such as India, Brazil and South Africa. Figure 4 compares these coalitions with the BRI and a residual category of "other" countries outside these defined groups.

Fig. 4: Scenario modeling: possible investment coalitions



Own illustration and data analysis. Data scraped from: SemiconductorEngineering website.

The results in Figure 4 reveal significant differences in investment capacity depending on how coalitions are formed. On its own, a narrow EU coalition lags significantly behind the rest of the world, highlighting the impact of fragmentation within the EU, where divergent state aid policies and uncoordinated national initiatives dilute collective financial strength. In such an environment, the BRI emerges as a strong contender, leveraging China's central coordination and financing capabilities.

[92] See: https://www.bloomberg.com/news/articles/2024-10-24/tsmc-s-arizona-chip-production-yields-surpass-taiwan-s-a-win-for-us-push.

However, if the EU extends its partnerships to a Western coalition, this coalition clearly dominates global investment, reflecting the combined economic and strategic resources of its member states. A broader Democracy Coalition would have an even clearer lead. This analysis underlines the need for the EU to strengthen internal cohesion through mechanisms such as the IPCEIs and permanent frameworks such as the GBER. It also highlights the importance of leveraging partnerships with trusted global allies. Only through such a balanced approach can the EU reduce its dependence on external systems and establish itself as a leading player.

6. While the EU has traditionally focused on consumer welfare as the primary objective of its competition policy, the digital age has brought new competition-related challenges that require a more nuanced approach. The "New Brandeisian" approach in the US, championed by scholars such as Lina Khan and possibly also embraced by the Trump 2.0 administration, represents a significant shift from the traditional consumer welfare standard.[93] This movement argues for a broader view of antitrust that takes into account factors such as market structure, worker protection, and the preservation of small businesses. For example, the EU could consider incorporating elements of New Brandeisian thinking into its competition framework, such as giving greater weight to the long-term effects of mergers on innovation and market structure.[94] However, it is crucial that the EU strikes a balance that maintains legal certainty and does not discourage legitimate business activity. International cooperation networks play an important role in addressing these challenges. The European Competition Network (ECN), which facilitates cooperation between the Commission and national competition authorities, provides a model for effective cross-border enforcement. To address the sketched trade-off between consumer welfare and wider public interests, the EU could propose the creation of a specialised working group within the International Competition Network (ICN).

5 Conclusion: The hierarchy of trade-offs

Digital policy analysis often gets bogged down in intricate detail, leading to a fragmented understanding that overlooks the broader implications and interconnectedness of different policy objectives. This compartmentalised approach can obscure the inherent trade-offs but also potential synergies between different policy areas. Due to current geopolitical pressures – exacerbated by recent developments such as the Trump 2.0 presidency – there is an increased need to adopt a holistic perspective that takes into account the complex interplay between competitiveness, security, and fundamental rights. In this paper, we have provided a conceptual framework for doing so by conceptualising a trilemma in EU digital policymaking. This trilemma states that contrary to common rhetoric, the EU cannot simultaneously maximise economic competitiveness and innovation, ensure security and sovereignty, and fully respect fundamental rights and social cohesion without making compromises.

Each case study we examined illustrates the concrete manifestations of this trilemma: 1. The GDPR enhances individual privacy but imposes compliance costs that may hinder innovation and competitiveness, especially for SMEs. 2. The DSA aims to create a safer digital environment but raises concerns about freedom of expression and imposes regulatory burdens that could affect the competitiveness of platforms. 3. Initiatives such as the 5G Security Toolbox and cloud certification schemes prioritise security and sovereignty, but may strain economic relations with key technology providers, affecting

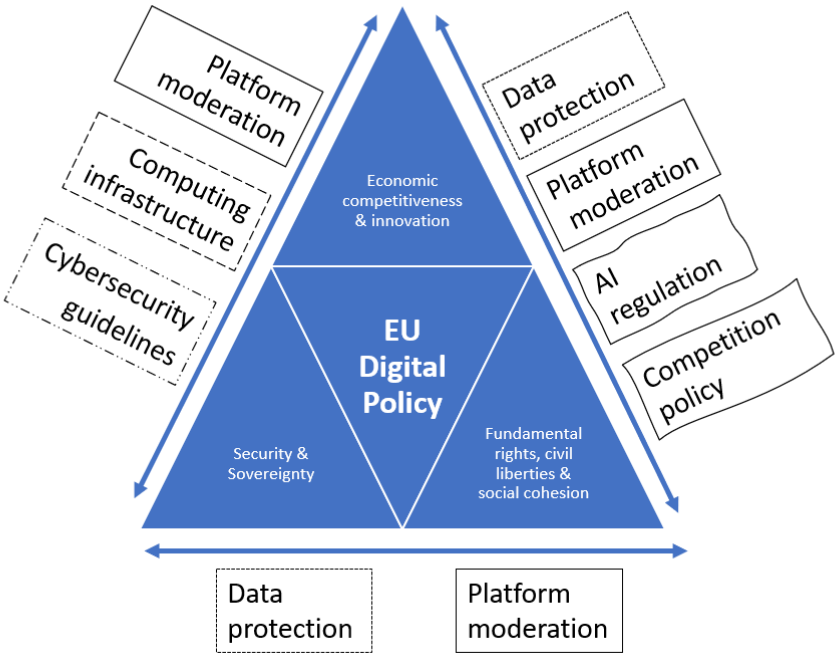
[93] Lina Khan, 'The New Brandeis Movement: America's Antimonopoly Debate', *Journal of European Competition Law & Practice* 9, no. 3 (1 March 2018): 131–32, https://doi.org/10.1093/jeclap/lpy020.

[94] Florian Kraffert, 'Should EU Competition Law Move Towards a Neo-Brandeis Approach?', *European Competition Journal* 16, no. 1 (2 January 2020): 55–96.

short-term competitiveness. 4. The AI Act seeks to set ethical standards for AI development, which may increase compliance costs and impact innovation, balancing fundamental rights with economic competitiveness. 5. Efforts such as the EU Chips Act and AI Factories aim at strategic autonomy but may lead to inefficient resource allocation and internal market distortions, reflecting a trade-off between sovereignty and economic efficiency. 6. The evolving role of EU competition policy could take into account broader societal concerns beyond consumer welfare, such as climate change or security, but could lose sight of its original objective as formulated in the Treaties and become too discretionary.

Aggregating our findings and linking them back to our original framework (Figure 5), these case studies show that all digital and technology policies are united by the presence of strong trade-offs that are not always explicitly acknowledged. The trilemma framework allows us to map these trade-offs along the three axes of competitiveness, sovereignty, and fundamental rights. It becomes clear that some policies involve more trade-offs than others. For example, data protection involves two sides of the trilemma, while platform moderation cuts across all three dimensions, suggesting a hierarchy of complexity in policymaking. This hierarchical understanding may have implications for current plans to harmonise and streamline EU digital policy. Recognising the different degrees of trade-offs allows policymakers to prioritise issues that require a more nuanced balancing act, and to design policies that are more coherent. Acknowledging the trilemma also encourages more dialogue between different DGs and stakeholders. More generally, the new EU Commissioner for Tech Sovereignty, Security and Democracy should be aware that no single policy approach can adequately address all concerns without potentially compromising other goals. To foster a resilient digital ecosystem, the EU must explicitly recognise and quickly address these trade-offs and allow for policy learning over time.

Fig. 5: Summary of results



Own illustration.

In the final section of this paper, we have suggested a way of addressing some of the trade-offs through a route that has become less popular in recent years – international cooperation. While the pursuit of strategic autonomy has become a dominant theme in recent EU digital policy, our analysis suggests

that international cooperation remains an important avenue for mitigating the inherent trade-offs identified in the tech policy trilemma. For example, international cooperation offers opportunities to balance privacy and innovation by harmonising data protection standards, as seen in different adequacy agreements. In platform moderation, collaboration with democratic allies can help develop best practices that protect freedom of expression while enhancing security. On cybersecurity, partnerships with technologically advanced nations can strengthen the EU's defences without undermining economic interests, e.g. through joint R&D projects with Israel. On AI regulation, participation in global fora such as the Global Partnership on Artificial Intelligence allows the EU to promote ethical standards without isolating itself from international innovation networks. In the area of computing infrastructure, strategic alliances can help the EU achieve its goals without inefficient allocation of resources, as demonstrated by TSMC's collaboration with the US. Finally, in competition policy, international networking can help balance consumer welfare with broader public interests by ensuring that EU competition law enforcement takes into account global dynamics without becoming too discretionary or isolated. Therefore, while strategic autonomy remains important, a balanced strategy involving global partnerships is essential to harmonise and streamline EU digital policies and mitigate some of the trade-offs inherent in the tech trilemma.

Centrum für Europäische Politik
FREIBURG | BERLIN

Authors:

Dr. Anselm Küsters, LL.M.
Head of Division Digitalisation and New Technologies
kuesters@cep.eu

Dr. Cecilia Emma Sottilotta
Assistant Professor of Political Science, University for Foreigners of Perugia (Unistrapg)
cecilia.sottilotta@unistrapg.it

Centrum für Europäische Politik FREIBURG | BERLIN
Kaiser-Joseph-Straße 266 | D-79098 Freiburg
Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin
Tel. + 49 761 38693-0

The **Centrum für Europäische Politik** FREIBURG | BERLIN, the **Centre de Politique Européenne** PARIS, and the **Centro Politiche Europee** ROMA form the **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Free of vested interests and party-politically neutral, the Centres for European Policy Network provides analysis and evaluation of European Union policy, aimed at supporting European integration and upholding the principles of a free-market economic system.