Politics and Governance
2025 • Volume 13 • Article 10331
https://doi.org/10.17645/pag.10331

cogitatio

ARTICLE

Open Access Journal

EU Data Sovereignty: An Autonomy–Interdependence Governance Gap?

Helena Carrapico [1] and Benjamin Farrand [2]

[1] Social Sciences Department, Northumbria University, UK
[2] Law School, Newcastle University, UK

Correspondence: Helena Carrapico (helena.farrand-carrapico@northumbria.ac.uk)

Submitted: 14 March 2025 **Accepted:** 14 May 2025 **Published:** 16 July 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

The EU has explicitly linked the concept of data sovereignty to its ambitions as an international regulatory agenda-setter in its position as self-described geopolitical union. In particular, the EU has expressed repeatedly its desire to ensure its strategic autonomy, reducing its dependence on third countries and their key industries. The purpose of this article is to explore EU data governance ambitions by highlighting the gap between those autonomy aspirations and the reality of data interdependence on the ground. More specifically, through the framework of the "autonomy-interdependence" governance gap, the article proposes to analyse the clash between the EU's desire to ensure autonomy and the inherently interdependent nature of data flows between states, and its dependence on non-EU data servers. Using the case study of semiconductor supply chains, this article analyses the data dimension of this EU-designated critical technology, and the flows of information relating to the research, design, and fabrication of these chips. Considering the EU's attempts to control data under its Data Act and Data Governance Act, it argues that the EU will have considerable difficulty in operationalising these data sovereignty ambitions, particularly as they relate to ensuring that all data stays within the EU, or within its sphere of regulatory influence.

Keywords

data localisation; data sovereignty; European Union; interdependence; semiconductors; strategic autonomy

1. Introduction

The concept of digital/technological sovereignty has become a central pillar of the EU's technological and industrial policies, reflecting a growing ambition to assert control over critical digital infrastructures, data

flows, and technological standards. As discussed below, the Commission uses the two terms, digital sovereignty and technological sovereignty, interchangeably, and for this reason, we have chosen to frame this as "digital/technological" sovereignty, which encapsulates the broader sovereignty aims of the Commission's policies in technology governance. Against the backdrop of escalating geopolitical tensions, technological rivalries, and vulnerabilities exposed by the Covid-19 pandemic, the EU has increasingly framed digital/technological sovereignty as essential to its economic resilience, security, and global leadership (Carrapico & Farrand, 2020; Farrand et al., 2024). As highlighted in Thierry Breton's statement that "Europe may have lost the battle to create digital champions capable of taking on US and Chinese companies harvesting personal data, but it can win the war of industrial data" (Breton, 2020, as cited in "Europe can win global battle," 2020), the concept of data sovereignty is central to the digital/technological sovereignty agenda, encompassing the control and governance of data generated, processed, and stored within the EU and by its stakeholders. Furthermore, increased autonomy and presence in semiconductor supply chains, are seen by the EU as essential to securing this sovereignty as the essential building blocks of digital technologies (European Commission, 2022a). Data sovereignty is intricately tied to the EU's broader vision of digital autonomy, forming the basis for initiatives that aim to develop a robust European data economy and establish the EU as a global norm-setter in data governance. While these ambitions are reflected in strategic documents such as the European Strategy for Data and the European Chips Act, the challenges in implementing the EU's ambitions expose its dependence on global supply chains and external actors. This article examines the feasibility of the EU's data sovereignty ambitions by exploring the case study of the semiconductor industry—a critical and highly interconnected sector underpinning the digital economy and security. Semiconductor data plays a key role at every stage of the supply chain, from research and design to manufacturing and distribution. However, the industry's complexity and reliance on transnational networks highlight the tension between the EU's aspirations for autonomy and the realities of interdependence, effectively underscored by Monsees (2025).

To explore this tension between expectations and outcomes, the article starts by discussing its proposed analytical framework, the EU's data autonomy-interdependence gap, which enables us to evaluate the EU's data sovereignty initiatives against political, legal, and operational criteria, both internally and externally. As will be explained in Section 2, the theoretical framework takes inspiration from Christopher Hill's capability—expectations gap; where he highlighted that the EU's capabilities (as an international actor) had been promoted to the point where an important gap between its capabilities and expectations had emerged (Hill, 1993), which was starting to impact the EU's practices and outcomes as an international actor. Similarly to Hill, the authors hope to bring a much-needed reality check, in this case, to the field of data governance. The remainder of the article applies the analytical framework to the EU semiconductor data governance case study: Section 3 explores the EU's data governance expectations by focusing on its ambition for this area, and Section 4 contrasts the EU's rhetoric with its implementation by considering whether the outcomes are in line with expectations. In doing so, the article aims to shed light on the EU's role in shaping the future of global data governance and reflects on the broader implications for the EU's digital/technological sovereignty agenda and its wider geopolitical ambitions. Methodologically, the authors make use of thematic analysis of European Commission and European Union Council documents published between 2018 and 2024 to, first, identify trends in EU ambitions and, second, to analyse subsequent governance practices. Overall, the authors propose to contribute to the fast-growing academic literature focusing on the EU as a cybersecurity actor (Christou, 2015; Dunn Cavelty, 2013; Farrand et al., 2024; Obendiek & Seidl, 2023) by exploring the sub-field of data governance. Although it constitutes a key aspect

of cybersecurity, and it has received substantial attention in science and technology studies (see for example Bellanova & Glouftsios, 2022), it remains severely underexplored within the international relations literature.

2. Digital/Technological Sovereignty and the EU: Is There a Gap Between Expectations and Outcomes?

In this section, we outline the EU's digital/technological sovereignty ambitions and how they link to the concept of data sovereignty, before outlining the analytical framework used to explore the autonomy-interdependence gap. The first von der Leyen Commission made digital/technological sovereignty central to its technology-related policies, whether they relate to technical standards, the protection of democracy online, or green energy policies. Despite using the terms "digital" and "technological" sovereignty interchangeably (Bellanova et al., 2022), the Commission identified the key purpose of digital/technological sovereignty as an initiative aimed at ensuring Europe's autonomy by reducing technological dependencies on the rest of the world, reinforcing the EU's ability to define its own rules and values, and asserting those rules and values as the basis for cooperation with those outside of its borders (European Commission, 2020d, p. 3). As such, the study of the EU's digital/technological sovereignty initiatives has become the significant focus of a number of academics working on EU policies, ranging from considerations of industrial policy (Seidl & Schmitz, 2023), cybersecurity (Farrand et al., 2024) and internal market regulation (Heidebrecht, 2024), to discrete policy areas such as artificial intelligence (Calderaro & Blumfelde, 2022) and reflections on normative implications for European governance (Floridi, 2020; Thumfart, 2024). Digital/technological sovereignty is subsequently becoming a core element of EU relations with the external world, as well as an internal motivator for action. The second von der Leyen Commission has established a new mandate around the concept, with the creation of an Executive Vice President for Tech Sovereignty, Security and Democracy. In the mission letter outlining the brief, von der Leyen stated that this sovereignty agenda was central to guaranteeing Europe's global leadership and its security, resilience, and future (von der Leyen, 2024b, p. 6).

A key element of this is "data sovereignty." As with "technological" sovereignty, there are some indications that at least some users of the terms do so interchangeably (see Hummel et al., 2021). Data sovereignty may be distinguished from digital/technological sovereignty insofar as it relates specifically to control over data, whether through data protection law, competition law, or national security law, and thereby can be considered a subcategory of digital/technological sovereignty (Chander & Sun, 2023, p. 7). For the Commission, data infrastructure was identified as a core component of digital/technological sovereignty in the Shaping Europe's Digital Future communication (European Commission, 2020d, p. 3), with data becoming "a key factor of production…we need to build a genuine European single market for data—a European data space based on European rules and values" (European Commission, 2020d, p. 5). However, concern was also raised about the market power of large players referred to as "big tech," based outside of the EU's borders (European Commission, 2020d, p. 5). In this communication, we are able to see both an internal and an external dimension to data sovereignty, combining the desire to build European infrastructure akin to an "internal" industrial policy and to ensure that data outside of the EU's borders is governed by European rules and values, representing an "external" leadership ambition focused on setting global standards (see Farrand et al., 2024). The concept of data sovereignty builds upon the perceived strengths of the EU as a regulatory power, first considered in the context of the protection of *personal* data under the General Data Protection Regulation (GDPR) as representing a "Brussels effect," in which the EU is able to dictate the terms of global standards for data regulation without needing explicit forms of cooperation or coercion (Bradford, 2021).

However, as this article explores, while this may have been arguable in the context of the personal data of EU citizens in the geopolitical context in which the GDPR was enacted, the EU is not necessarily as powerful on the world stage as previously argued, and data sovereignty efforts are instead motivated by a sense of insecurity based on a perception that the EU is at a competitive disadvantage with countries such as the US and China (European Commission, 2020a; see also Farrand & Carrapico, 2022). In this context, there is the potential for the EU's data sovereignty ambitions to be unrealised due to a gap between the EU's desires for autonomy and its ability to reduce external interdependencies.

As mentioned in the Introduction, the article explores the EU data governance's autonomy–interdependence gap by developing an analytical framework that takes inspiration from Hill's capability—expectations gap (Hill, 1993), as well as from previous work carried out on EU cybersecurity policy (Carrapico & Farrand, 2024). By taking this analytical route, the authors are consciously favouring a pre-theoretical and more pragmatic approach, which they hope will be of use for the development of future theoretical development. Hill focuses on both *actorness* and *presence* to understand what kind of international actor the EU is, conceptualising the EU's role through its various activities in the world. Actorness as an international actor entails being delimited from others, autonomous in the sense of making its own laws and decisions, and possessing legal personality, diplomatic agents, and the ability to conduct negotiations with third parties (Hill, 1993). Presence emphasises the EU's "variable and multidimensional presence" in international affairs (Hill, 1993, p. 309), yet where our approach diverges is that Hill argues that presence is used to "get [the author] off the hook of analysing [European Political Cooperation] in terms of sovereignty and supranationalism" (Hill, 1993, p. 309), whereas we instead incorporate the Commission's sovereignty discourse and supranational actions into the analysis in order to demonstrate how it promotes an understanding of the EU's desires of autonomy as a sovereignty actor that has a feasibility gap in terms of the EU's interdependencies in the studied field. Similarly to Hill's work, the article maps the rhetorical ambitions of the EU and contrasts them with the pattern of EU activity that has been observed. More specifically, given the article's focus on the feasibility of the EU's data sovereignty ambitions, the authors propose to identify political, legal, and operational criteria to ascertain whether EU ambitions are shared, enforceable, or implementable, both within the EU and in its relations with third countries (see Table 1). Where the political criteria are concerned, the framework asks, overall, whether the EU ambitions of data autonomy are clearly expressed and shared among EU actors and EU member states, as well as whether there are possible obstacles or incentives to these ambitions. The legal criteria interrogate the existence of legal instruments in this field and whether they are enforceable. Finally, the operational criteria questions the extent to which EU data ambitions are being implemented by private actors and third countries, and whether existing critical infrastructures and data supply chains can support such autonomy ambitions. As discussed in the Introduction, we shall explore this specifically using the case study of data flows for semiconductor research, design, and fabrication.

3. The EU's Autonomy Ambitions in the Area of Data Governance

To assess the autonomy–independence gap in EU data sovereignty, it is necessary to first outline what ambitions the EU has in this field, as they relate to the political, legal, and operational criteria. The political ambitions of the Commission can be found in the European Strategy for Data (European Commission, 2020b), which was published shortly after Shaping Europe's Digital Future. It is worth mentioning that the EU had already demonstrated a desire to develop a common European data space in 2018, but this was

Table 1. EU data sovereignty–autonomy–interdependence gap framework.

	Internal dimension	External dimension
Political criteria	• Is the EU's data sovereignty ambition clearly stated in political documents? Does this ambition align itself with broader EU objectives, such as digital/technological sovereignty? • Are the EU's data sovereignty ambitions shared among EU institutions and EU member states? Are the ambitions supported by a shared understanding of data sovereignty? • What are the political obstacles/incentives among EU institutions and EU member states?	• Is the EU's data sovereignty ambition towards third countries clearly stated in political documents? • Are the EU's data sovereignty ambitions towards third countries shared among EU institutions and EU Member States? • What are the political obstacles/incentives regarding exporting EU data sovereignty norms and standards? • Do existing policies address data sovereignty norms and standards for exporting to third countries? Have those policies been co-created with third countries?
Legal criteria	• Do legal instruments reflect data sovereignty ambitions? • Do legal instruments contain clear and enforceable legal provisions?	• Do legal instruments reflect the EU's data sovereignty ambitions towards third countries? • Do legal instruments contain clear and enforceable legal provisions towards third countries?
Operational criteria	• Are private actors implementing EU ambitions and policies? • Is critical infrastructure able to support EU data sovereignty ambitions? • Are EU data supply chains compatible with EU data sovereignty ambitions? • Are there mechanisms to monitor policy implementation?	• Are third countries adopting EU norms and standards? • Are third countries' critical infrastructure able to support EU data sovereignty ambitions? • Are international data supply chains compatible with EU data sovereignty ambitions? • Are there mechanisms to monitor EU policy implementation in third countries?

framed solely in economic terms, rather than in security or sovereignty terms (European Commission, 2018). By way of comparison, and while the European Strategy for Data is still concerned with economic benefits, security and sovereignty are identified as being central to the EU's survival and are explicitly linked to actions in the fields of personal data protection and cybersecurity, with the EU positioned as vulnerable to the advanced levels of competitiveness of the US "free market" and the Chinese "state surveillance" models of Big Tech development (European Commission, 2020b, p. 3). Therefore, the political ambition in data governance is based explicitly on ensuring EU digital/technological sovereignty in enabling data technologies and infrastructures. There is an element of internal industrial policy through creating infrastructures that allow for the EU's share of the data economy, "data stored, processed and put to valuable use in Europe—at least corresponds to its economic weight, not by *fiat* but by choice" (European Commission, 2020b, p. 4). There is also an element of external norm setting through "building upon the strength of the Single Market's regulatory environment [to shape] global standards and [create] an

environment in which economic and technological development can thrive, in full compliance with EU law" (European Commission, 2020b, p. 23). Furthermore, as former Commissioner Breton made clear, initiatives in the context of ensuring data sovereignty have been focused on industrial data, classified as any non-personal data, and having significant commercial value (European Commission, 2020b, p. 1). Of particular relevance to the semiconductor industry, beyond manufacturing, sales, and other forms of "logistical" data is intellectual property (considered as industrial data), whether in the form of copyright schematics, typographical circuit information, patents, or trade secrets (Farrand, 2025).

As a result of these ambitions, legal responses are strongly based on the logic of "data localisation," in which there is an emphasis on retaining data within a country or region's geographical control (Fratini & Musiani, 2024). Two legislative proposals around this have been central to the EU's ambitions: The first was a Proposal for a Data Governance Act (European Commission, 2020c) and the second was a Proposal for a Data Act (European Commission, 2022c). The Data Governance Act was intended to make data sharing easier in the EU area and it was implemented as Regulation 2022/868. This Regulation facilitates the re-use of public sector data and eases the transfer of data shared between businesses, including where that data is non-personal and protected by confidentiality or intellectual property rights (Article 3 of the Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022, 2022). Data intermediation services, which offer services by which data holders can make the data available for potential data users are able to offer those services under Article 10, and they can be based outside of the Union so long as they agree to abide by EU law and appoint a representative in an EU member state under Article 11. Under Article 12, these services are obliged to ensure that where data may be processed outside of the EU, specify the third-country jurisdiction in which the data use is intended to take place, allowing for opt-outs from this usage (Article 12(n)). Furthermore, all services are obliged to take all required measures to prevent international transfer or governmental access to non-personal data held in the Union, where such transfer or access would create a conflict with Union law under Article 31. The Data Act, adopted as Regulation 2023/2854 goes further; it applies its laws to any products or services made available in the Union regardless of where the service or product supplier is based under Article 1 and it places a specific emphasis on non-access by third countries. Under Article 32, strict limits are placed on data transfer to third countries, or requests to access EU data (including non-personal data) by third countries, with requests only being permitted where they are considered proportionate, legitimate, and compliant with EU law. This has been identified as important in restricting the ability of third countries or actors within them being able to access sensitive industrial data of importance to the EU's economic and security interests (European Commission, 2020b, p. 9). It also seeks to facilitate internal data interoperability as a means of fostering a common European Data Space (Article 33). A key intention behind the Data Act is to provide extra-territorial reach, particularly in light of the dependence upon American and Chinese companies providing cloud-based data-storage servers (Casolari et al., 2023). With this in mind, digital/technological sovereignty may be considered as the underlying rationale for the interpretation and application of the Act (Ryan et al., 2024).

In terms of practical operationalisation of this ambition to create more European services in the context of a European Data Space, and reduce dependency on external suppliers, the Commission proposed some concrete steps. Internally, this is focused on increasing the attractiveness of the EU as somewhere for data to be based. This includes infrastructure investment and support for European cloud services and member state initiatives such as Gaia-X (European Commission, 2020b, pp. 15–17), launching an EU cloud marketplace (European Commission, 2020b, pp. 18–19), as well as promoting the development of Common European

Data Spaces in areas of strategic economic sectors, with manufacturing identified as one of the key areas for providing investment and common governance models (European Commission, 2020b, pp. 21–22). Furthermore, the EU intends that creating these favourable conditions would "attract the storage and processing of data from other countries and regions" (European Commission, 2020b, p. 24), in essence operationalising increased levels of data localisation within EU territory. Where this is not feasible, the EU instead states the ambition of ensuring that any access or use of EU personal or non-personal data is done on the basis of EU rules and values (European Commission, 2020b, p. 23), working through multinational fora so as to "promote the European model around the world" (European Commission, 2020b, p. 24). Along these lines, the EU has concluded a Joint Declaration on a Digital Alliance with Latin America, with data governance, security, and infrastructure forming part of its informal dialogue remit (European Union & Latin America and Caribbean, 2023, p. 2), as well as having concluded an EU–Singapore Digital Trade Agreement in July 2024, which facilitates cross-border transfers of data and an agreement not to unjustifiably enforce data localisation requirements (European Commission, 2024a). However, the effectiveness of these activities is open to question, as will be discussed in the next section, using the case study of semiconductor data supply chains to identify the gaps between promoting autonomy and continued interdependence.

4. The Interdependence Dilemma and Unfeasible Ambitions: The Case Study of Semiconductor Data

This final section of the article considers the EU data governance's autonomy–interdependence gap by exploring the case study of semiconductor data. It does so, firstly, by introducing why this case study is well-placed to challenge the EU's data sovereignty ambitions, and, secondly, by applying the analytical framework presented in Section 2 (see Table 1).

4.1. Semiconductor Data: A Case Study on Complexity and Interconnectedness

The control of industrial data for semiconductor supply chains is a particularly interesting case study, not only given the centrality of microchips in powering almost everything in contemporary society, but also due to their high level of supply chain complexity, specialisation, and interdependence. Semiconductors are materials, such as silicon or germanium, that can conduct electricity and that can be processed to create intricate circuit designs, which we commonly call chips. Chips power all modern electronic devices, ranging from microwaves to calculators, from smartphones to intercontinental ballistic missiles (Orton, 2009). The semiconductor industry is therefore central to the EU's digital/technological sovereignty, given that "there is no digital without chips" (von der Leyen, 2021, p. 4). For the Commission, the EU's digital/technological sovereignty is entirely dependent upon guaranteeing its supply of microchips and the resilience of its semiconductor supply chains (European Commission, 2022a, p. 22). This, in turn, is intended to secure the EU's autonomy and sovereignty in associated technological fields. However, the production of microchips is dependent upon industrial research data, which may be protected as trade secrets or as intellectual property rights (Hoeren, 2016). For this reason, the security of this data is critical. As highlighted by Khan et al. (2021), global semiconductor supply chains, which are currently evaluated at half a trillion dollars, are highly dispersed and see individual chips in production crossing an average of 70 international borders, with multiple companies feeding into the process of their production. Whereas considerable semiconductor research takes place in the US and the EU, the raw materials that are used to produce EU semiconductors (silicon, gallium, and germanium) mainly stem from China, Russia, Japan, and Germany,

where they are refined and cleaned of impurities. The raw materials are then transformed into wafers, which serve as the base for semiconductors, in facilities mainly located in South-East Asia, in particular South Korea, Taiwan, and Malaysia, as well as the US and China. The wafers are then used to design integrated circuits, whose market is led by American, Japanese, and Chinese companies ("Semiconductor manufacturing facilities," 2024). The production of the manufacturing equipment is also a particularly important element of the supply chain, with the EU, the US, and Japan being responsible for most of the manufacturing equipment. The wafers containing the designed circuits are then cut into individual microchips, assembled, and packaged into different final technological products. This phase of the supply chain mainly takes place in Taiwan, South Korea, the US, Germany, The Netherlands, France, and Ireland (Council of the European Union, 2022). For the EU, this sector has been valued at €52.1 billion (European Semiconductor Industry Association, 2022). The EU has large firms involved in the research and design of microchips and controls over IP, such as Extoll (Germany) and Menta (France), as well as being a key provider of tools such as lithography devices for production through ASML (based in the Netherlands). However, this data and these tools are then exported to third countries, such as TSMC in Taiwan and Samsung in South Korea. It has integrated device manufacturers (that design and manufacture their own semiconductor chips for use in their own devices) but these are almost exclusively limited to the automobile industry (European Semiconductor Industry Association, 2022).

The data dimension of the semiconductor supply chain mirrors its manufacturing complexity, involving numerous types of data (Ji et al., 2023; TSMC, n.d.), such as (a) research data (produced in universities, businesses, and governmental centres); (b) the proprietary data concerning the design and architecture of the chip; (c) material and equipment data integration (the quality of raw materials, delivery schedules, and equipment performance); (d) manufacturing and production data (photolithography, etching and wafer testing, as well as data analytics on the optimisation of the production process); (e) quality control and testing data (chip defects and their origin); (f) logistics and distribution data (inventory levels, shipping routes, and delivery times); and (g) customer feedback and performance monitoring data (product performance and usage). This type of supply chain generates enormous datasets, which feed into different elements of the manufacturing of semiconductors and evolve throughout the lifespan of the supply chain. This data then requires the necessary infrastructure to be stored safely, processed, and analysed (Mönch et al., 2018).

Looking at the semiconductor supply chain as a whole, three immediate challenges emerge regarding EU data sovereignty: (a) the development of EU infrastructures that are safe and able to store, process, and analyse this volume of data; (b) the difficulty in determining the data owner given the transborder complexity of the supply chain and the cumulative nature of semiconductor data; and (c) the dependence on non-EU data and data infrastructures, which is linked to the absence of the EU from large parts of the supply chain. These challenges highlight the interconnected and transnational nature of semi-conductor data and question whether the EU's ambitions of data autonomy are at all realisable. The following sub-section of the article reflects on these questions by applying the autonomy–interdependence gap framework discussed in Section 2 (see Table 1).

4.2. The Internal and External Dimensions of the Autonomy–Interdependence Gap

As mentioned in Section 2, the article's framework foresees the application of three criteria (political, legal, and operational) to the EU's internal and external dimensions of data sovereignty governance, as understood specifically through the lenses of EU semiconductor data (see Table 2).

Where the challenges in the context of the internal dimension are concerned, there is an indication that the data sovereignty ambition is clearly stated in a considerable range of EU political documents. From the European Strategy for Data (European Commission, 2020b) to the Digital Compass 2030 (European Commission, 2021) and the European Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023, 2023), the EU presents a united front on the centrality of data in driving economic innovation and security, and on the need to regulate how ever-growing quantities of data are stored, processed, and utilised in line with EU priorities. The European Chips Act reflects this same level of prioritisation for semiconductor data, which it presents as being central to achieving digital/technological sovereignty (European Commission, 2022b). Semiconductor data is understood as having a key role in the research, design, and manufacturing of technology, as well as in identifying vulnerabilities in supply chains and fostering trust among stakeholders. It is also perceived as being instrumental in enhancing the EU's ability to bridge the gap between advanced semiconductor research and sustainable industrial application while reducing dependence on third countries and contributing to achieving the EU's aim to double its global semiconductor production share from 10% to 20% by 2030. The Council and the Parliament share this enthusiastic support for semiconductor data, as can be seen from the Member States' Declaration on Processors and Semiconductor Technologies (European Commission, 2020e), as well as from the Council and the Parliament's limited changes to and absence of resistance to the Commission's proposal for the EU Chips Act (Kleinhans, 2024).

From a legal perspective, the European Chips Act introduces the necessary provisions to align semiconductor data governance with broader data sovereignty ambitions (as expressed in the Data Act and Data Governance Act). The regulation establishes mechanisms to monitor and secure semiconductor data flows and imposes obligations on stakeholders to ensure data security and interoperability. It also seeks to ensure full protection of confidential information and intellectual property rights under Article 33. Combined with the Data Act and Data Governance Act, this framework provides for a well-defined set of provisions intended to ensure data sovereignty, with recital 43 of the Chips Act making clear the concerns regarding data accessed from outside the Union and the need to reduce dependencies on external states and sectors. However, the enforceability of these provisions is open to question. In fact, a number of member states are currently subject to Commission proceedings for not complying with the Data Governance Act's requirement to provide an oversight body (European Commission, 2024b). Furthermore, as will be discussed below, with regard to operationalisation, the complexity of semiconductor supply chains makes full oversight of data flows exceptionally difficult to achieve. The EU has recently funded a Common European Data Space for manufacturing (Data Space 4.0), which has as a semiconductor research and design project (Chips Joint Undertaking) aiming at securing sovereignty in this field (Chips JU, n.d.). Another initiative is the European Processor Initiative, which has financed the French company SiPearl to design microprocessors for high-performance computing. However, SiPearl only engages in research and design, as manufacturing takes place in Taiwan (SiPearl, 2023), presumably necessitating data outflows.

Regarding the operationalisation of EU data governance, and despite the apparent political alignment, questions remain about whether the EU's ambitions for semiconductor data sovereignty are shared uniformly among member states and institutions. While member states largely support the idea of reducing dependence on third-country suppliers, divergences have emerged over implementation strategies, particularly concerning resource allocation and the role of state aid (Poitiers & Weil, 2024). For example, member states with strong semiconductor industries, such as Germany, France, and the Netherlands, have

advocated for aggressive investments in research and development, while others, with fewer capabilities, have expressed concerns about the equitable distribution of EU funds (Haeck, 2022). Furthermore, there has been additional disagreement as to where the €43 billion necessary to deliver on the EU's ambition to transform the semiconductor landscape will come from. In this context, the Council of the European Union voted unanimously in 2022 to prevent the Commission from using Horizon Europe's leftover funds to support the Chips for Europe Initiative—which was created by the European Chips Act (Tani & Zubascu, 2022). This financial uncertainty has also been made worse by the private sector's cautious approach to investing in the EU semiconductor industry, despite the Commission's announcement that EU funding would be accompanied by large-scale private investment. In 2024, for example, Intel decided to shelve and delay a number of important investments, including a €30 billion semiconductor factory in Germany and a €5 billion production facility in Poland (Haeck, 2024). These divergences point to a potential misalignment in operationalising the shared vision of data sovereignty.

Additional operational challenges further exacerbate the autonomy–interdependence gap. While initiatives such as the EU Chips Joint Undertaking and European Data Spaces, including the project Gaia-X, aim to enhance the EU's semiconductor and data infrastructure, progress has been uneven. The lack of pan-European coherence in infrastructure development has led to fragmentation, with member states prioritising national projects over collective efforts. Moreover, while EU-based semiconductor firms, like ASML and STMicroelectronics, play a significant role in specific segments of the supply chain, their global operations often depend on non-EU partners for critical components, raw materials, and advanced manufacturing equipment. Similarly, the EU continues to be over-reliant on non-EU companies' investment in order to increase its semiconductor production capacity. It is the case, for example, of the creation, in 2024, of the European Semiconductor Manufacturing Company (ESMC), a joint venture between the Taiwan Semiconductor Manufacturing Company and three EU companies (Bosh, Infineon, and NXP). ESMC is currently in the process of building a semiconductor production facility in Dresden, which will be 70% owned by the Taiwanese company (Iskyan, 2024). These different forms of interdependence may enable the expansion of semiconductor production, but they also complicate efforts to achieve true data autonomy, as a significant portion of semiconductor data may be generated, processed, or stored outside EU jurisdiction.

Regarding the external dimension, the EU's ambition to export its regulatory approach also encounters significant geopolitical challenges. While the EU Chips Act and the broader European Strategy for Data emphasise the importance of establishing global norms, the EU faces competition from the US and China, which pursue their own regulatory and industrial strategies. The US CHIPS and Science Act, for instance, offer substantial subsidies to domestic semiconductor firms, creating competitive pressure for EU companies that rely on transatlantic partnerships. In addition, the US has, since the start of 2025, been pursuing a more aggressive semiconductor strategy: the Biden administration made the decision to limit the export of artificial intelligence semiconductors on security grounds, affecting 17 member states (Haeck, 2025); and the Trump administration has actively encouraged semiconductor companies to relocate their production facilities to American territory through the threat of increased tariffs (Mariani, 2025). Similarly, China's state-driven semiconductor strategy prioritises self-sufficiency, making it less receptive to adopting EU standards. China has its own "cyber sovereignty" ambitions (Jiang, 2010; Shen, 2016) that are heavily based on controlling data outflows, as well as exporting its own approach to data governance through its agreements and infrastructure support for other states through initiatives such as the Digital Silk Road (Hussain et al., 2024). Furthermore, in the face of increasing trade hostility from the US, China is seeking to

develop its own advanced chip production capacities, facilitated through significant investments at home and increased cooperation in East Asia (Kim & Rho, 2024). Additionally, while the EU has engaged in bilateral and multilateral initiatives to promote its data sovereignty norms, these efforts have had mixed results. Agreements such as the EU–Singapore Digital Trade Agreement demonstrate a willingness among third countries to align with EU principles, but the absence of similar agreements with major players like the US and China, each seeking to support its own ambitions in this sector, limits the EU's influence in shaping global semiconductor data governance. Finally, the fragmented nature of global supply chains makes it difficult for the EU to monitor compliance with its rules once semiconductor data leaves its jurisdiction.

Table 2. EU data sovereignty–autonomy–interdependence gap applied to the EU semiconductor case study.

	Internal dimension	External dimension
Political criteria	• The EU's semiconductor data sovereignty ambitions are clearly stated in political documents and this ambition aligns itself with broader EU objectives • EU's semiconductor data ambitions are shared among EU institutions and EU member states. Understanding of data sovereignty is, however, vague and often used interchangeably with digital/technological sovereignty • No political obstacles have been identified	• The EU's semiconductor data sovereignty ambition towards third countries is clearly stated in political documents • The EU's semiconductor data sovereignty ambitions towards third countries are shared among EU institutions and EU member states; • No political obstacles have been identified
Legal criteria	• Legal instruments set out obligations for the protection of industrial data • While provisions appear clear, questionable ability to enforce	• Legal obligations codify approach to data sovereignty vis-à-vis third countries • Enforcement dependent upon internal dimension, extraterritoriality of regulation difficult to achieve
Operational criteria	• Operationalisation reveals divergence among member states regarding resource allocation • Disagreement between member states and Commission as to the source of the funding for this area • The private sector has adopted a cautious approach and investment has been limited	• The EU has a limited number of agreements with third countries covering semiconductor data. There is therefore a limited number of countries adopting EU norms and standards • EU's influence in shaping global semiconductor data governance is quite limited • The fragmented nature of global supply chains makes it difficult for the EU to monitor third-country compliance

5. Conclusion

The article proposed examining the EU's ambitions for data sovereignty through the lens of semiconductor data, using the autonomy–interdependence gap framework in order to assess whether the EU's political, legal, and operational initiatives match up with its ambitions. It argued that while the EU has established a clear vision for data sovereignty, buttressed by strategic policies and regulatory tools, such as the European

Data Act and the European Chips Act, it is faced with considerable challenges in operationalising its ambitions. While the EU seeks to ensure autonomy, its ability to do so is hindered by the extent of interdependence in semiconductor production. Internally, inconsistencies among member states in terms of funding, investment in infrastructure, and industrial strategy have cast uncertainty over the EU's capacity to muster a coherent and unified approach to this field. Externally, the highly transnational and interdependent nature of semiconductor supply chains has exposed the EU's continued dependence on third countries for raw materials, technology, and investment. Further, the EU's leverage over global data governance norms is limited in the face of alternative regulatory visions from the US and China. Overall, this case study identifies the broader complexities in the EU digital/technological sovereignty agenda. While the EU hopes to become a regulatory leader, its global influence in semiconductor data governance is subject to it being able to negotiate geopolitical competition, secure critical supply chains, and balance its autonomy ambitions with the realities of interdependence. At a greater level of generality, the control of data relevant to semiconductor development is reflective of a broader potential autonomy–interdependence gap in the pursuit of the EU's data sovereignty goals. The feasibility of increasing data localisation and reducing dependency on third-country services is questionable given the high levels of interdependence in industrial data flows, particularly where research, design, production, and distribution, are all steps in supply chain processes that take place in different states. The Commission has not yet produced its new Union Data Strategy, announced in the context of the von der Leyen II political guidelines (von der Leyen, 2024a), yet we argue that greater recognition of the complexities that interdependence creates in the pursuit of autonomy should be explicitly addressed. In terms of future research, we consider that expanding the analysis to different sectors in which data interdependence, or other forms of interdependence, is a predominant characteristic would help to further reinforce the findings regarding the autonomy–interdependence gap in the EU's pursuit of its digital/technological sovereignty ambitions.

Acknowledgments

We would like to thank the academic editors, Dr Xuechen Chen and Dr Xinchuchu Gao, for their efforts in organising this thematic issue, and for their helpful comments during the drafting stages. We would also like to thank all the participants in the thematic issue workshop, which took place in January 2025, for all their comments and questions.

Funding IM

Publication of this article in open access was made possible through the institutional membership agreement between the Northumbria University and Cogitatio Press.

Conflict of Interests

The authors declare no conflict of interests.

References

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Bellanova, R., & Glouftsios, G. (2022). Formatting European security integration through database interoperability. *European Security*, *31*(3), 454–474. https://doi.org/10.1080/09662839.2022.2101886

Bradford, A. (2021). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: The case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111–1126. https://doi.org/10.1080/07036337.2020.1853122

Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *JCMS: Journal of Common Market Studies*, *62*(S1), 147–158. https://doi.org/10.1111/jcms.13654

Casolari, F., Buttaboni, C., & Floridi, L. (2023). The EU Data Act in context: A legal assessment. *International Journal of Law and Information Technology*, *31*(4), 399–412. https://doi.org/10.1093/ijlit/eaae005

Chander, A., & Sun, H. (2023). Introduction: Sovereignty 2.0. In A. Chander & H. Sun (Eds.), *Data sovereignty: From the digital silk road to the return of the state* (pp. 1–31). Oxford University Press. https://doi.org/10.1093/oso/9780197582794.003.0001

Chips JU. (n.d.). *Our vision*. https://www.chips-ju.europa.eu/Our-vision

Christou, G. (2015). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Palgrave Macmillan.

Council of the European Union. (2022). *The semiconductor ecosystem—Global features and Europe's position*. https://www.consilium.europa.eu/media/58112/220712-the-semiconductor-ecosystem-global-features-and-europe-s-position.pdf

Dunn Cavelty, M. (2013). *A resilient Europe for an open, safe and secure cyberspace* (Working paper No. 23). Swedish Institute of International Affairs.

Europe can win global battle for industrial data, Breton says. (2020, February 17). *Euractiv*. https://www.euractiv.com/section/digital/news/europe-can-win-global-battle-for-industrial-data-breton-says

European Commission. (2018). *Towards a common European data space* (No. COM(2018) 232). https://digital-strategy.ec.europa.eu/en/news/communication-towards-common-european-data-space

European Commission. (2020a). *2020 strategic foresight report: Charting the course towards a more resilient Europe* (No. COM(2020) 493). https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report_en

European Commission. (2020b). *A European strategy for data* (No. COM(2020) 66). https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission. (2020c). *Proposal for a regulation on European data governance* (No. COM(2020) 767). https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

European Commission. (2020d). *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en

European Commission. (2020e). *Joint declaration on processors and semiconductor technologies*. https://digital-strategy.ec.europa.eu/en/library/joint-declaration-processors-and-semiconductor-technologies

European Commission. (2021). *2030 digital compass: The European way for the digital decade* (No. COM(2021) 118 final/2). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118

European Commission. (2022a). *A Chips Act for Europe* (No. COM(2022) 45). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

European Commission. (2022b). *Proposal for a regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)* (No. COM(2022) 46). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0046

European Commission. (2022c). *Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act)* (No. COM(2022) 68). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0068

European Commission. (2024a). *Agreement on digital trade between the European Union and the Republic*

of Singapore—Working text. https://www.bilaterals.org/IMG/pdf/eu-singapore_text_of_the_digital_trade_agreement.pdf

European Commission. (2024b, December 16). *Commission calls on 10 Member States to comply with the Data Governance Act | Shaping Europe's digital future* [Press release]. https://digital-strategy.ec.europa.eu/en/news/commission-calls-10-member-states-comply-data-governance-act

European Semiconductor Industry Association. (2022). *Welcome to ESIA*. https://www.eusemiconductors.eu/esia

European Union & Latin America and Caribbean. (2023). *Joint declaration on a digital alliance*. https://international-partnerships.ec.europa.eu/document/download/15512057-a80d-4428-bf34-24608adfb0e4_en?filename=EU-Latin_America_and_Caribbean__Joint_Declaration_on_a_Digital_Alliance.pdf

Farrand, B. (2025). The economy–security nexus: Risk, strategic autonomy and the regulation of the semiconductor supply chain. *European Journal of Risk Regulation*, *16*(1), 279–293. https://doi.org/10.1017/err.2024.63

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs*, *100*(6), 1–24.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Fratini, S., & Musiani, F. (2024). Data localization as contested and narrated security in the age of digital sovereignty: The case of Switzerland. *Information, Communication & Society*. Advance online publication. https://doi.org/10.1080/1369118X.2024.2362302

Haeck, P. (2022, November 15). In the global chips race, EU's cash engine sputters. *Politico*. https://www.politico.eu/article/budget-squabbles-put-eu-on-the-back-foot-in-the-chips-race

Haeck, P. (2024, September 17). The EU's chips plan implodes as Intel pauses investments. *Politico*. https://www.politico.eu/article/intel-germany-chips-plant-competitiveness-eu-ambition

Haeck, P. (2025, January 14). US limits on AI chips split EU. *Politico*. https://www.politico.eu/article/eu-warns-back-against-us-artificial-intelligence-chip-export-china-limits

Heidebrecht, S. (2024). From market liberalism to public intervention: Digital sovereignty and changing European Union digital single market governance. *JCMS: Journal of Common Market Studies*, *62*(1), 205–223. https://doi.org/10.1111/jcms.13488

Hill, C. (1993). The capability-expectations gap, or conceptualizing Europe's international role. *Journal of Common Market Studies*, *31*(3), 305–328.

Hoeren, T. (2016). The semiconductor chip industry—The history, present and future of its IP law framework. *International Review of Intellectual Property and Competition Law*, *47*(7), 763–796.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 1–17. https://doi.org/10.1177/2053951720982012

Hussain, F., Hussain, Z., Khan, M. I., & Imran, A. (2024). The digital rise and its economic implications for China through the digital Silk Road under the Belt and Road initiative. *Asian Journal of Comparative Politics*, *9*(2), 238–253. https://doi.org/10.1177/20578911231174731

Iskyan, K. (2024, September 3). TSMC starts building its first European chip plant. *Global Finance Magazine*. https://gfmag.com/technology/tsmc-chip-plant-germany

Ji, K., Nauta, L., & Powell, J. (2023). *Mapping global supply chains—The case of semiconductors*. Rabobank.

https://www.rabobank.com/knowledge/d011371771-mapping-global-supply-chains-the-case-of-semiconductors

Jiang, M. (2010). Authoritarian informationalism: China's approach to internet sovereignty. *SAIS Review of International Affairs*, *30*(2), 71–89.

Khan, S. M., Mann, A., & Peterson, D. (2021). *The semiconductor supply chain: Assessing national competitiveness*. Center for Security and Emerging Technology. https://doi.org/10.51593/20190016

Kim, Y., & Rho, S. (2024). The US–China chip war, economy–security nexus, and Asia. *Journal of Chinese Political Science*, *29*(3), 433–460. https://doi.org/10.1007/s11366-024-09881-7

Kleinhans, J.-P. (2024, July 30). *The missing strategy in Europe's chip ambitions*. Interface. https://www.interface-eu.org/publications/europe-semiconductor-strategy

Mariani, M. (2025). *Trump's proposed tariffs on semiconductors*. Z2Data. https://www.z2data.com/insights/impact-report-trumps-proposed-tariffs-on-semiconductors

Mönch, L., Uzsoy, R., & Fowler, J. W. (2018). A survey of semiconductor supply chain models part I: Semiconductor supply chains, strategic network design, and supply chain simulation. *International Journal of Production Research*, *56*(13), 4524–4545. https://doi.org/10.1080/00207543.2017.1401233

Monsees, L. (2025). The paradox of semiconductors—EU governance between sovereignty and interdependence. *Cambridge Review of International Affairs*, *38*(1), 3–21. https://doi.org/10.1080/09557571.2024.2405915

Obendiek, A. S., & Seidl, T. (2023). The (false) promise of solutionism: Ideational business power and the construction of epistemic authority in digital security governance. *Journal of European Public Policy*, *30*(7), 1305–1329. https://doi.org/10.1080/13501763.2023.2172060

Orton, J. W. (2009). *Semiconductors and the information revolution: Magic crystals that made IT happen*. Academic Press.

Poitiers, N., & Weil, P. (2024, November 12). *Is the EU Chips Act the right approach?* Bruegel. https://www.bruegel.org/blog-post/eu-chips-act-right-approach

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). (2022). *Official Journal of the European Union*, L 152/1. https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). (2023). *Official Journal of the European Union*, L 2023/2854. http://data.europa.eu/eli/reg/2023/2854/oj/eng

Ryan, M., Gürtler, P., & Bogucki, A. (2024). Will the real data sovereign please stand up? An EU policy response to sovereignty in data spaces. *International Journal of Law and Information Technology*, *32*(1), Article eaae006. https://doi.org/10.1093/ijlit/eaae006

Seidl, T., & Schmitz, L. (2023). Moving on to not fall behind? Technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy. *Journal of European Public Policy*, *31*(8), 2147–2714.

Semiconductor manufacturing facilities map. (2024, May 27). *Technology in Global Affairs*. https://technologyglobal.substack.com/p/semiconductor-manufacturing-facilities

Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review*, *1*(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

SiPearl. (2023). *SiPearl*. https://sipearl.com/european-processor

Sjostedt, G. (1977). *External role of the European Community*. Lexington Books.

Tani, C., & Zubascu, F. (2022, December 1). EU ministers stop €400M of decommitted Horizon Europe money

being diverted to the Chips Act. *Science|Business*. https://sciencebusiness.net/news/eu-ministers-stop-eu400m-decommitted-horizon-europe-money-being-diverted-chips-act

Thumfart, J. (2024). *The liberal internet in the postliberal era: Digital sovereignty, private government, and practices of neutralization*. Palgrave Macmillan.

TSMC. (n.d.). *A look at semiconductor supply chains—Taiwan semiconductor manufacturing company limited*. https://www.tsmc.com/english/aboutTSMC/dc_infographics_supplychain

von der Leyen, U. (2021). *2021 state of the Union address by President von der Leyen: Strengthening the soul of our Union* (No. SPEECH/21/4701). European Commission. https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701

von der Leyen, U. (2024a). *Europe's choice: Political guidelines for the next European Commission*. https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf

von der Leyen, U. (2024b). *Mission letter to Henna Virkkunen, Executive Vice-President-designate for tech sovereignty, security and democracy*. European Commission. https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf

About the Authors

Helena Carrapico is a professor of international relations and European politics at Northumbria University. Her research is centrally concerned with addressing how internal security concerns, including cybersecurity, are constructed, represented, and responded to by different actors, as well as how those responses impact society at large. She hopes that one day her love of watching science fiction and her love of research may be unified.

Benjamin Farrand is a professor of law and emerging technologies at the Newcastle University Law School. His research focuses on the interactions between law and politics in the regulation and governance of new technologies, including in fields such as cybersecurity and online platforms. It also focuses on the interactions between academic scholarship and caffeine intake, which requires continuous experimentation.