Received: 15 February 2023 | Accepted: 26 July 2023

DOI: 10.1002/poi3.358

RESEARCH ARTICLE

P&I Policy & Internet PSO WILEY

The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem

Filippo Gualtiero Blancato

Department of Computer Science, University College London, London, UK

Correspondence

Filippo Gualtiero Blancato, Department of Computer Science, University College London, London, UK.
Email: Filippo.blancato.21@ucl.ac.uk

Funding information

Engineering and Physical Sciences Research Council, Grant/Award Number: EP/S022503/1 - project reference 2576186

Abstract

How does the European Union balance the need to migrate data to the cloud with the imperative of reducing its dependence on foreign cloud providers? Cloud computing is a critical technology for the competitiveness of the European Union (EU) in the digital economy. This paper argues that the EU is adopting a host of regulatory requirements and industrial policy tools—which fall under the umbrella term of 'data sovereignty'—not only to protect the confidentiality of European data, but also to counter the dominance of US vendors in the European cloud market. To demonstrate how data sovereignty principles are woven into current EU policy initiatives, the paper presents two case studies: Gaia-X and the European Alliance for Industrial Data, Edge, and Cloud. Linking data sovereignty to the lack of a competitive European cloud ecosystem sheds light on the strategic dimension of cloud computing in a way that treating them separately would not do.

KEYWORDS

cloud computing, data sovereignty, Edge, European Alliance for Industrial Data, European Union, Gaia-X

INTRODUCTION

Much of today's geopolitics revolves around industrial policy. Recent breakthroughs in digital technologies promise to accelerate developments in a variety of sectors at an unprecedented pace. According to some, these developments will have as transformational

an impact as general purpose technologies of the past, such as printing, steam, and electricity (Coyle, 2021, p. 169; Helpman, 1998). Considering the weight of such revolution, the competitive advantage enjoyed by states that will harness such technologies is expected to have a profound impact on their ability to act in the international stage. The United States and China have already devised strategies to achieve primacy in sectors such as 5G, cloud computing, and artificial intelligence. Conversely, polities like the European Union (EU) are scrambling to catch up against their competitors while addressing strategic dependencies. Against this background, this paper focuses on the EU approach to cloud computing, a technology which has emerged as a key enabler for the digital economy, and whose sustained adoption among private companies is rapidly spilling over to the public sector.

Cloud computing is widely regarded as being the future of computing (Schneier, 2019). Relying on computing-as-a-service allows both businesses and institutions to cut the upfront costs of investing in their own data centres and only pay for the storage and features offered by vendors. Moreover, cloud providers can be expected to provide better security than the majority of companies they serve, thanks to their scale and technical expertise.[1] Considering the above, one should not be surprised to learn about the continuous growth of the cloud market. Estimates point at a public cloud spending growth of 20.4% in 2022, from $410.9bn in 2021 to $494.7 bn in 2022, with predictions that spending might reach almost $600 bn in 2023 (Gartner, 2022). In Europe alone, the cloud market was worth around EUR 53bn in 2021 and is set to grow to EUR 300 bn in 2030 (OVHCloud, 2021). Yet, contrary to countries such as the United States and China, Europe is lagging behind in the development of its cloud capabilities. The vast majority (92%) of data produced in the West is stored in US servers (Propp, 2019). Moreover, the Directorate General for Communications, Content, and Technology in the European Commission quantifies an investment gap—measured as a difference between what the United States and China and the EU invest, including public and private investments—at EUR 11bn per year in cloud computing (European Commission, 2021b). It is also estimated that US cloud providers invest 10 times more in research and innovation in cloud computing than what their EU competitors do (European Commission, 2021b).

The issue of European dependence on foreign cloud providers has received scarce academic attention so far. Where academic sources focus on cloud computing, they do so either from a technical, economic, or legal vantage point (Alouffi et al., 2021; Hon et al., 2016; Kushida et al., 2015), with only perfunctory attention devoted to its broader strategic implications. The paper addresses this research gap by placing European initiatives on the cloud in the context of a wider policy agenda seeking to revive the competitiveness of the European industrial ecosystem in digital technologies. To do so, it draws from the analysis of official publicly available policy documents. These include: strategies, regulations, and staff working documents (SWD) released mainly by the European Commission; declarations and announcements by cloud computing companies; and documents outlining the vision and organisational features of industrial initiatives such as Gaia-X and the European Industrial Alliance on Data, Edge and Cloud.[2]

Drawing from these sources, this study maintains that the EU is pursuing a data sovereignty agenda to offset the lack of competitiveness of its European cloud ecosystem. Cloud computing is characterised by significant economies of scale, and non-European hyperscalers[3] have readily captured increasing shares of the European market, de facto confining local players to niche areas. According to European policymakers, the fact that the majority of European data is stored in servers operated by on-European companies that are subject to extra-territorial legislations makes such data potentially accessible by third countries. Data sovereignty principles can require European governments to choose vendors that are not subject to any extraterritorial legislation. As such, they can reduce the space of action of American providers in the European market. In this sense, while data

sovereignty demands aim to tackle legitimate security concerns about the confidentiality of European data, they can also be considered part of an EU industrial policy agenda to catch up in the development and deployment of enabling technologies. Linking data sovereignty to the lack of competitive European cloud service providers (CSPs) sheds light on the strategic dimension of cloud computing in a way that treating them separately would not do.

The rest of the paper is structured as follows: the first section provides an overview of the basic characteristics of cloud computing and its strategic dimension. The second section briefly discusses the EU regulatory approach to the cloud sector and measures the concentration of the European cloud market. This is instrumental to understand the industrial policy rationale of the EU data sovereignty agenda, which is discussed in the third section. Finally, the fourth section of the paper presents two case studies: Gaia-X and the European Alliance on Industrial Data, Cloud, and Edge. Their analysis suggests that the EU is relying on both 'open' and 'exclusive' industrial policy initiatives to push its data sovereignty agenda and close the gap with American CSPs.

THE STRATEGIC DIMENSION OF THE CLOUD: A BRIEF OVERVIEW

The present phase of technological transformation is premised on the gradual digitalisation of nearly every process. The European Commission estimates that the volume of global data will increase by 530% between 2018 and 2025, from 33 zettabytes to 175 (European Commission, 2020b). This means that, in a digital economy, the volume of data produced will be such that their storage in on-premise servers might not always be a feasible solution (for a competing argument, see Wang & Casado, 2021). Thus, cloud computing is rapidly becoming a critical component of companies and governments' digital transformation.

Cloud computing is a platform service for storing, managing, and processing data on a remote rather than on local servers (for a technical definition, see Mell & Grance, 2011). In this sense, it is an evolution of the internet infrastructure, and contains both a hardware component (or 'physical' layer) and a software component (or 'abstraction' layer). The physical layer consists of servers, storage, and network components like routers and switches, but also firewalls. The abstraction layer is the software that is deployed across the physical layer to facilitate access to—and engagement with—the physical layer (Mell & Grance, 2011, p. 2). A visual representation of the cloud's layers is provided in Figure 1.

There are three main types of cloud services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Each of these services entails a

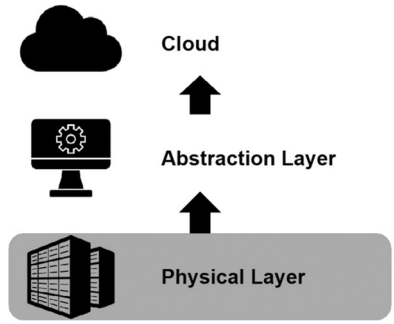

FIGURE 1 The physical and abstract layer in the cloud. *Source*: Author's elaboration.

greater level of abstraction than the previous one. An overview of cloud computing services and deployments is provided in Supporting Information: Appendix I.

Since its inception, cloud computing has known a very rapid diffusion (Byrne et al., 2018). It is even suggested that the adoption of cloud computing is so widespread, and its services so indispensable, that the technology will rapidly evolve into a form of utility (Carr, 2008; for a different perspective see Kushida et al., 2011). One reason for the attractiveness of the cloud is that it allows customers—whether public or private—to significantly reduce or even eliminate the upfront costs of investing in expensive in-house data centres. Moreover, the cloud offers flexibility and scalability in that customers have access to a shared pool of computing resources with a 'pay-as-you-go' model and can adapt workloads according to their needs. While not void of vulnerabilities (Alouffi et al., 2021), the Cloud also offers security advantages in terms of resilience and redundancy, since data are stored in multiple data centres to prevent data loss in case of cyberattacks, outages, and natural disasters.

As observed by Herr, the cloud now 'influences the trajectory of nations and the conduct of statecraft' (2020a. 2020b, 25). This is because the cloud is at the heart of a technological continuum encompassing 5G networks, Internet of Things (IoT), and artificial intelligence, which are all enabled by advanced computing power capabilities. Therefore, countries that harness cloud computing can potentially benefit from a comparative advantage in the development of a wide array of technologies. All this bears an impact not only on economic competitiveness, but also on geopolitical competition. A recent study by Mueller and Farhat (2022) corroborates this view by mentioning cloud computing as one of the sectors of the digital economy whose domestic market processes the United States and China are trying to influence as part of their competition for hegemony. The authors label such predicament 'digital neomercantilism'.

The strategic dimension of the cloud has pushed European countries to scramble for its adoption while preserving the security of their data. In 2020, representatives of EU Member States signed a joint declaration to accelerate the development of a European cloud infrastructure for businesses and the public sector (Joint Declaration on Cloud, 2020). Meanwhile, European national governments enacted 'Cloud first' policies to facilitate a rapid and secure migration of their data to the Cloud. In May 2021, France launched a National Strategy for the Cloud based on five priorities (Stratégie Nationale Pour le Cloud, 2021). It also approved a series of requirements enshrined in the label 'SecNumCloud' (or Cloud de Confiance), developed by the French Agency for the Security of Information Systems (ANSSI) to enhance data sovereignty through cybersecurity standards and techno-economic criteria against extra territorial legislations. Similarly, Italy launched its Cloud First Policy in September 2021 (ACN, 2021), while already in January 2020 Germany had updated the C5 Criteria Catalogue, which defines a baseline security level for cloud computing (BSI, 2020). Such policy initiatives attest to the reality that a partial migration of public sector's data to the Cloud is inevitable because of the inherent benefits provided by this platform service. Yet the governmental approach to cloud computing is not confined to reasons of economic efficiency. The sensitivity of governments' data, coupled with a strict data protection regime, make data security a key part of the EU's approach to cloud computing. More importantly, the significant economies of scale of the cloud market make it difficult for European CSPs to establish themselves as credible alternatives to the sophisticated and relatively cheap offerings of American CSPs.

THE EU REGULATORY APPROACH TO THE CLOUD SECTOR

The previous section has provided a definition of cloud computing and touched upon its strategic dimension. This section briefly discusses the EU regulatory approach to the cloud sector, as well as its concentration. Measuring market concentration sheds light on the very

limited weight that European cloud providers carry in this sector. This is unequivocally spelled out in documents such as the EU Strategy for Data, which maintains that 'EU-based cloud providers have only a small share of the cloud market, which makes the EU highly dependent on external providers […] and subject to a loss of investment potential for the European digital industry in the data processing market' (66 Final. 2020). More importantly, making sense of the lack of competitiveness of European CSPs is a critical prerequisite to understand the industrial policy rationale of the data sovereignty agenda pursued by the EU.

From an economic perspective, concentration in the cloud market is not necessarily concerning. Current incumbents might enjoy large market shares because of their efficiency or the superiority of their products. Also, concentration in the cloud is partly driven by intrinsic characteristics of the market, which is capital-intensive due to high upfront costs and R&D investments required to enter and compete, economies of scale that ultimately benefit incumbents, intense price competition, and low-profit margins that discourage new entrants. This explains, to some extent, the greater shares of the market enjoyed by American hyperscalers compared to their European competitors. Furthermore, unlike the United States, the European digital market is fragmented along national market lines, making it more difficult for European enterprises to scale up and compete. Cloud adoption in Europe is also much slower than in the United States: while just 41% of companies in the EU have migrated to the cloud, with significant differences between member states (Eurostat), 94% of enterprises in the United States use at least one type of cloud deployment (Forrester, 2022).

The characteristics of the cloud market, however, do not shield it from competition concerns. As mentioned above, the dominance of American cloud providers and the economies of scale they enjoy represent significant barriers to entry and expansion and can effectively prevent European vendors from challenging their entrenched position. Although the application of traditional competition law to cloud computing has been slow (for a comprehensive account, see Gleeson & Walden, 2021), the EU is increasingly leveraging its regulatory powers to devise a toolkit that can effectively force competition in the European cloud sector. For instance, the stated purpose of the Digital Markets Act (DMA) is to manage the market power of large online platforms, including cloud providers. These are considered among the 'core platform services' acting as 'gatekeepers', that is as 'gateways […] between business users and end users, and enjoy an entrenched and durable position […] which reinforces existing entry barriers' (DMA, 2020, p. 1. see also Lundqvist, 2019). The Digital Services Act (DSA), which regulates the provision of 'intermediary services' in the internal market, refers to cloud computing providers as both hosting services and online platforms. Finally, one of the objectives of the draft EU Data Act is to foster competitiveness in cloud computing by enforcing 'data portability', meaning the possibility for users to move their data from one cloud provider to another, thus making it easier to switch providers and avoid vendor lock-in (Data Act, 2022).[4] While these may seem as purely competition policy initiatives, they are consistent with a wider industrial policy agenda. In fact, Since competition policy is one of the few exclusive competences of the Union, it is not surprising to see the EU pursuing other strategic industrial policy objectives through competition policy means.

According to some, the EU regulatory toolkit has several shortcomings and is guilty of lumping together different online services while failing to consider the specific characteristics of the cloud sector. Specifically, it has been argued that the DMA defines cloud providers platforms even if they do not really intermediate between businesses and users; similarly, the DSA imposes on cloud providers obligations that are meant for online platforms, thus creating an unnecessary regulatory burden; finally, the Data Act is too broad in scope (Geradin et al., 2022). Others, instead, have wondered whether initiatives like the Data Act, in trying to counter the dominance of large-scale US cloud giants, might create an 'unnecessary regulatory straightjacket' that ultimately prevents European businesses from

reaping the benefits of the data economy (Renda, 2022). Beyond the antitrust debate about the feasibility and the modalities of regulating the cloud, however, it is clear that the strategic dimension of this digital infrastructure makes governments weary of excessive dependence on foreign providers, ultimately prompting greater regulatory scrutiny. In fact, the challenges posed by the digital economy have revived the European debate about whether competition policy should help meet industrial policy objectives rather than technocratic assessments of consumer welfare (on this debate, see Lianos, 2019).

Measuring concentration

For the purpose of measuring its concentration, the European Commission establishes that a relevant market is defined by product and geographical location (European Commission 2004). With regard to the first, measuring cloud concentration should focus on the three main layers of the cloud, that is IaaS, PaaS and SaaS. This is not always feasible due to the fact that cloud providers use different definitions for the various layers of the cloud and record them in different ways. As an alternative, one can consider a combination of the three. With regard to geography, we use data gathered by the Dutch Competition Authority (ACM)[5] on the state of the EU cloud market in 2020 (Table 1).[6]

To gauge the competitiveness of the EU cloud market we use a common measure of market concentration, the Herfindahl–Hirschman Index (HHI). This is computed as the sum of the squared market shares of the firms in a given market. Squaring market shares allows to give more weight to larger firms and hence obtain a more precise estimate of market power. Based on figures from Table 1, the HHI of the EU cloud market ranges from 2500 to 3450.[7] This corresponds to the description of a highly concentrated market, as shown in Table 2.

Similar conclusions are drawn by other estimates, which show that, with the notable exception of France—where local provider OVH is third—AWS, Azure, and Google Cloud are the three dominant CSPs in Europe (Table 3). When considering the evolution of the American hyperscalers' shares in Europe, between 2021 and 2022, market data shows an increase from 66% to 72% (Synergy Group, 2022).

These results, however, refer to the three cloud layers combined. More granular data on the level of public cloud market concentration in western Europe[8] shows that, while at the IaaS layer the market is very concentrated, with AWS, Microsoft, and IBM jointly commanding 58% of the shares, the PaaS layer is more moderately concentrated, with 55.5% of the market concentrated among four non-European companies (Microsoft, AWS, Salesforce and Google); finally, the SaaS layer is more fragmented with three companies

TABLE 1 EU market shares—all cloud layers combined (except productivity software)—2020.

Company	Market Share (%)
Amazon Web Services	35–40
Microsoft Azure	35–40
Google Cloud	5–10
Oracle	5–10
IBM	0–5
Others	0–5

Source: Authority for Consumers & Markets (ACM) (2022).

TABLE 2 Concentration levels, types of markets, and market power.

Level of concentration	Type of market	Market power	Herfindahl–Hirschman Index
Nonconcentrated market	Efficient competition, part of monopolistic competition	Low, if any	<1500
Moderately concentrated market	Part of monopolistic competition, loose oligopoly	Moderate	1500–2500
Highly concentrated market	Tight oligopoly, dominant firm	High	>2500

Source: Pavic et al. (2016).

TABLE 3 Cloud services leadership—Europe.

Rank	Total Europe	UK	Germany	France	Netherlands	Rest of Europe
Leader	Amazon	Amazon	Amazon	Amazon	Amazon	Amazon
#2	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft	Microsoft
#3	Google	Google	Google	OVH	Google	Google
#4	IBM	IBM	Deutsche Telekom	Orange	KPN	IBM
#5	Salesforce	Rackspace	IBM	Google	IBM	Salesforce
#6	Deutsche Telekom	Salesforce	Oracle	IBM	Oracle	Swisscom

Source: Synergy Group (2020).

(Microsoft, Salesforce and SAP) enjoying 20.6% of shares (European Commission, 2020, p. 13).

There is a crucial political dimension to concentration, namely that the biggest CSPs in the EU market are non-European. The leaders among European cloud providers are German companies SAP and Deutsche Telekom, each accounting for only 2% of the market (Synergy Group, 2022). Moreover, while the overall growth of the cloud market has allowed European providers to significantly increase their revenues between 2017 and 2022, their market shares have declined from 27% to 13% (Synergy Group, 2022). Such decline is in stark contrast with the rise of hyperscalers, whose unrivalled capital expenditure in European data centres and other critical components of the global cloud infrastructure allows them to capture increasing swaths of the market. As put by analysts, 'other cloud providers simply cannot match the scale and geographic reach of the big three market leaders [AWS, Microsoft, Google]' (Synergy Group, 2021b).

Despite calls by the European industry to increase cross-border strategic investments and harmonise EU rules, it is evident that the current rift between American and European CSPs makes the emergence of European challengers in the market highly improbable. Rather, the EU industry seems focused on capitalizing on the next waves of digital transformation, such as the cloud-edge continuum, to regain its competitiveness and provide offers built on top of the infrastructure of American players (European Industrial Technology Roadmap, 2021).

The market power of American CSPs is instrumental to appreciate the political rationale of the EU data sovereignty agenda. This, while tackling legitimate security concerns, also represents an industrial policy tool for the EU to boost the competitiveness of its cloud industry. The next section of the paper delves into the rationale of the EU focus on the

confidentiality of European data, as well as on its implications for the EU's industrial posture vis-à-vis the cloud.

DATA SOVEREIGNTY AND THE CLOUD

Data sovereignty can be defined as the idea that data should be subject to the laws and governance of the nation(s) where the data is collected (Hummel et al., 2021; For an institutional perspective on the concept of sovereignty, see Krasner, 1988). As such, data sovereignty is a subset of digital sovereignty, that is, the objective of maintaining or achieving an acceptable level of autonomy or independence in the use of digital technologies (Floridi, 2020). With an ever-greater amount of data stored and processed in the Cloud, data sovereignty has become a key priority for governments around the world. In other words, as put by Irion, data sovereignty is 'a concept that is attractive to governments because it holds the promise of striking a balance between the progressing virtualization of information and their undiminishing demand for exclusive authority and control' (Irion, 2012, p. 65).

The EU has placed great emphasis on the need for member states to consider the implications of migration to the Cloud for the security of their data (ENISA, 2011; European Commission, 2019, 2020a). As highlighted by a Commission's staff working document, 'the public cloud infrastructure market, largely overshadowed by the United States players […] raises concerns over the European cloud users' ability to maintain control over strategic and sensitive personal and nonpersonal data' (European Commission SWD 352 final, 2021b, p. 93). However, while the operations of foreign cloud providers in the EU may raise legitimate data protection concerns for policymakers, it is clear that the EU data sovereignty agenda is also geared towards 'gaining leadership in areas where the EU still lags behind' (European Commission, 2021b). In other words, to catch up with competitors like US hyperscalers. In this sense, it could be argued that data sovereignty is an integral part of an industrial policy toolkit through which European policymakers aim to somehow shield local companies from foreign competition.

There is no agreement, however, about whether data sovereignty requirements can boost privacy and security in the cloud. According to some, it is highly debatable that data sovereignty is worth pursuing at all in an age of transnational networks. Rather, the most effective way to reconcile a distributed network like the cloud with privacy would be to adopt technical safeguards such as encryption (Falknerath & Rosenzweig, 2012). The nature of the Cloud as a technology service, in fact, makes it challenging to ensure data is kept under the European data protection regime. This is mainly because the business of the largest cloud providers is inherently transnational, hence premised on cross-border data flows. When communicating online through e-mails or other instant messaging services, data can travel to servers outside a nation's border, even if the communication happens between two users residing in the same country (for a discussion see Hon et al., 2016). Moreover, data stored in the Cloud do not usually reside in a single data centre located in a specific territory under a given jurisdiction. Data can be moved around servers for technical and maintenance reasons, or can be copied and held in multiple locations to ensure redundancy and continuation of the service in case of malfunctioning or outages in one data centre. Given that the cloud market is dominated by CSPs with global reach that can rely on a global infrastructure, data challenges the very notion of territoriality that polities are now seeking to impress upon it (Daskal, 2015).

The existing tension between the governmental objective of keeping control over data flows and the cross-bordering nature of those very data flows echoes similar debates over the opportunity of bringing the governance of the Internet under the aegis of the nation-state

(Goldsmith & Wu, 2006; Mueller, 2017). In this perspective, the EU data sovereignty agenda is not dissimilar from comparable strategies adopted by the United States and China to achieve primacy in the governance of digital technologies. Much like the United States and China are decoupling their technology ecosystems and subsidising their industries, so the EU is capitalising on its regulatory capabilities to address strategic deficiencies in technologies like the cloud. This response to a more contested geopolitical environment should not come as a surprise, as digital sovereignty is a noncompetition objective and, as such, may yield anticompetitive results.

In security terms, the main proposition of the EU data sovereignty agenda is that European data can be exposed to the potential reach of extra-territorial legislations. Since, as shown above, the EU cloud market is largely dominated by US CSPs, the next section weighs in on the potential impact of American extra-territorial legislation, particularly the CLOUD Act, on the EU's data protection regime.

Data sovereignty and the US Cloud Act

The Clarifying Lawful Overseas Use of Data Act (Cloud Act) is a US federal law which maintains that American service providers, including cloud companies, must disclose all data in their possession—if so required by US legal authorities—regardless of the location of the data. The law amended the former Stored Communications Act (SCA) to allow US law enforcement authorities (LEAs) to access electronically stored data through a warrant, subpoena, or court order without the need to pass through traditional mutual legal assistance treaties (MLATs).[7] MLATs form the basis for international data sharing between LEAs, but have been considered too slow and challenging to use in the context of criminal investigations occurring under time constraints. The law was passed in 2018 as a consequence of a case involving the US government and Microsoft Corporation (the so-called Microsoft Ireland case) (for a comprehensive account, see Brier, 2017; Schwartz, 2018).

The main feature of the Cloud Act is that it follows a 'geography-agnostic approach to jurisdiction over cloud data' (Abraha, 2020, p. 332). As long as service providers are American, they are compelled to disclose data in their possession regardless of where the data is stored. As such, it sets a standard on foreign legislation interference which European policymakers consider dangerous for the confidentiality of European data. If American companies—so the argument runs—can be legally compelled to hand over data to US authorities regardless of their location, then the security of European data cannot be taken for granted. Moreover, the Act is in contrast with the provisions of the current European data protection regime, which restricts the transfer to third countries of data processed under European legislation. More specifically, article 48 of the General Data Protection Regulation (GDPR) clarifies that any request by a legal authority to transfer or disclose personal data cannot be accepted or enforced unless based on international legal agreements, such as MLATs, between the third country and the EU (see GDPR, 2018). In other words, European policymakers consider that data sovereignty can be compromised by legislations such as the CLOUD Act, which is predicated on the very purpose of bypassing traditional MLAT agreements. Thus, the key issue surrounding the potential impact of the CLOUD Act on EU legislation is concurrent jurisdiction. When American CSPs are compelled by their government to hand over data stored in EU data centres, should they hand it over and comply with the demands of the United States jurisdiction, thereby running the risk of breaching GDPR rules, with the consequent fines and reputational damage? Or alternatively, should they refuse to breach their GDPR compliance and, instead, run up against the US courts?

Such concerns have led the European Union to adopt a prudential approach regarding the effect of United States extra-territorial legislation. As specified in the EU Strategy on Data, 'while third country legislations like the US CLOUD Act are based on public policy reasons such as law enforcement access to data for criminal investigations, the application of foreign jurisdictions' legislation raises legitimate concerns for European businesses, citizens and public authorities over legal certainty and compliance with applicable EU law, such as data protection rules' (European Commission, 2020a, p. 9). According to some, however, these fears are largely inflated or inaccurate. For example, it is argued that the CLOUD Act does not enable US surveillance in Europe, since the Act only applies to court-authorised criminal investigations and does not provide the US government with any new authority to obtain content on national security grounds (BSA, 2021, p. 1; for an opposing view see Ionos, 2019). To address potential conflicts of law between the CLOUD Act and the GDPR, the EU has already entered formal negotiations with the United States to discuss an electronic evidence sharing agreement (European Commission, 2019). It is also argued that European concerns around US extra-territorial legislation are unfairly one-sided, since the EU itself disposes of legal instruments similar to the CLOUD Act to obtain data regardless of their location. The Council of the European Union, in fact, has recently reached an agreement with the European Parliament on the final draft of the Regulation on European Production and Preservation Orders (EPPO) European Commission (2018) to expedite the retrieval of electronic evidence in criminal investigation and bypass existing cumbersome MLATs requests, much like the CLOUD Act does (Council of the EU, 2023). Finally, the recent draft trans-atlantic data privacy framework (TADPF), reached in response to the invalidation of the Privacy Shield by the Court of Justice of the European Union, partially mitigates the security concerns posed by the CLOUD Act by limiting the access to data by US Intelligence authorities to what is 'necessary' and 'proportionate' to protect national security, as well as by establishing a redress mechanism for EU citizens to contest unlawful access to their data by US authorities (European Commission, 2022). As legal scholars have observed, a successful negotiation of the TADPF and the adoption of the EPPO Regulation might lead to a comprehensive EU–US agreement on cross-border data flows. This could significantly downsize, or even neutralize, the potentially disruptive impact of extra-territorial legislations such as the CLOUD Act on European privacy and security (Propp, 2022).

Yet even if such EU–US comprehensive agreement was brokered, it should not follow from this that the EU will abandon its data sovereignty agenda. Data sovereignty, in fact, does not only address security concerns about the confidentiality of European data. It also aims to create a space where European CSPs are able to develop notwithstanding competition by their American counterparts. In other words, the EU approach to data sovereignty does not merely reflect immediate security and privacy concerns. It also addresses long-term industrial policy objectives. In this regard, the Commissioner for the Internal Market Thierry Breton, who is in charge of the bloc's industrial policy, has clearly stated that the EU's ability to process data on European soil will be a crucial factor for its competitiveness in the development of emerging technologies (Bayart & Martin, 2018). Against this background, it is not surprising that the Declaration for building a federated European cloud infrastructure signed by EU Member States specifies that 'while all cloud providers are welcome in the European cloud federation, the resulting cloud capacities should not be subject to laws of foreign jurisdictions' (Joint Declaration on Cloud, 2020, p. 5). Similarly, EU regulations that aim to boost competition in the cloud sector also contain provisions to limit the impact of extra-territorial laws on European data. For instance, chapter VII of the draft Data Act foresees that 'providers of data processing services shall take all reasonable technical, legal, and organisational measures […] to prevent international transfer or governmental access to nonpersonal data held in the Union (Data Act, 2022, p. 54). Furthermore, early drafts of a European Cloud

Certification Scheme (EUCS) being elaborated by the European Union Agency for Cybersecurity (ENISA) suggest the certification might include 'immunity requirements' (Stupp, 2022). These are security restrictions mandating that data considered critical should be stored in cloud services run by European companies. All this demonstrates that the European emphasis on cloud providers being shielded from foreign laws is not only part of a broader push to escape US National Security Surveillance, but also a way to reinforce separate industrial policy initiatives to boost the competitiveness of the European cloud sector. Finally, these European initiatives mirror similar ambitions that some member states nurture at the national level. A French Senate report on digital sovereignty, for example, stresses the importance of 'promoting European cloud offerings that are differentiated by their level of trust' (Rapport n° 7 Sénat, 2019).

While it remains to be seen whether the EU data sovereignty agenda will manage to bolster the competitiveness of its cloud ecosystem, it has partially succeeded in shaping hyperscalers' offers to meet Europe's sovereignty demands. For example, Microsoft has pledged to create an 'EU Data Boundary', a set of initiatives to 'minimize transfers of both customer data and personal data outside of the EU […] to address the needs of European customers who are looking for even greater data localization commitments' (Smith, 2021), as well as a 'Microsoft Cloud for Sovereignty' targeted at public sector customers (Sanders, 2022). Similarly, AWS has announced a 'Digital Sovereignty Pledge' (Garman, 2022), while Google Cloud has devised 'Sovereign Solutions' to ease compliance with European regulations (Fox-Martin, 2022). The common denominator of the above initiatives is a commitment on data residency solutions, confidential computing, and various forms of advanced encryption.

This section has shown how the EU data sovereignty agenda is closely linked to industrial policy objectives. To illustrate how data sovereignty demands are being woven into industrial policy initiatives at the EU level, the next session delves into two case studies.

CASE STUDIES

This section illustrates the case studies of Gaia-X and the European Alliance for Industrial Data, Edge, and Cloud. The former represents a more open and inclusive industrial policy approach to cloud computing and data sovereignty. The latter a more exclusive and politically driven one.

GAIA-X

Gaia-X is an industry-led initiative that aims to increase the EU's resilience and autonomy in cloud computing. It was initiated by the German and French Finance ministers in June 2020 (Bmwk, 2019). Official documents state that the purpose of Gaia-X is the 'creation of a federated data infrastructure based on European values of data and cloud sovereignty' (see Gaia-X website). However, the organisation does not aim to create a European Cloud provider alternative to US hyperscalers. Rather, it works to create a network of cloud services operating through common EU protocols and in compliance with EU data protection rules. This should lead to the creation of an open, federated, secure, and trustworthy data and cloud infrastructure. As put by official documents, Gaia-X wants to shift from a 'concentrated, proprietary, opaque' traditional cloud to a 'distributed, open, transparent' architecture. As observed in its concept paper, 'European alternatives (to non-European corporations) do not offer any comparable market capitalisation, scalability or breadth of applications; they are active in specialist niches at best. There is a risk of European data

being stored outside of Europe or on servers in Europe that belong to non-European companies and will be subject to a so-called lock-in' (Gaia-X, 2020a, p. 5).

Behind Gaia-X are companies from different sectors. The project was initially joined by 22 founding members and, at the time of writing, is enlarged to 350 companies and organisations. Among these are American and Chinese companies, including cloud providers Salesforce, Snowflake, Oracle, IBM, Google Cloud, Amazon Web Services, Microsoft, and Alibaba; software company Palantir; security company Cisco; and telecommunications company Huawei (Gaia-X, 2021). Non-European companies are further represented through trade associations.

The participation of non-European members is described by Gaia-X proponents as functional to the achievement of its purposes. However, this has sparked protests due to the alleged surveillance practices of some companies and their belonging to national governments with data protection approaches that differ to those of the EU (Goujard, 2021). To benefit from the contribution of leading players in foreign markets while shielding the organisation from excessive foreign influence, its management has attempted to put in place appropriate safeguards. As a result, non-European companies can become members of Gaia-X, but their voting rights are limited. Moreover, they can contribute to the policy rules committees, data spaces committees, and technical working groups, but the Board of Directors, in charge of steering the overall direction and priorities of the organisation, is composed solely of European companies. Figure 2 details Gaia X's organisational structure.

Gaia-X works to promote interoperability (the ability of computer systems to communicate and work together) and data portability (the possibility of moving one's data from one provider to another without constraints). As noted by the organisation's CEO, 'The leading Digital Platforms use proprietary, noninteroperable technologies that present concerns of control and lock-in' (Bonfiglio, 2021, p. 9). This is in line with concerns expressed by European companies which, in a report addressed to European internal market commissioner Thierry Breton, note:

> Once a company or a public administration has a large amount of data within one Cloud provider, it is very difficult and costly, both in technical and economic terms, to move data to another provider. When building a new product, it is relatively easy to adopt the latest innovative cloud solution. But migrating an existing data and business logic to a new cloud solution remains technically and financially challenging. (European Industrial Technology Roadmap, 2021, p. 13)

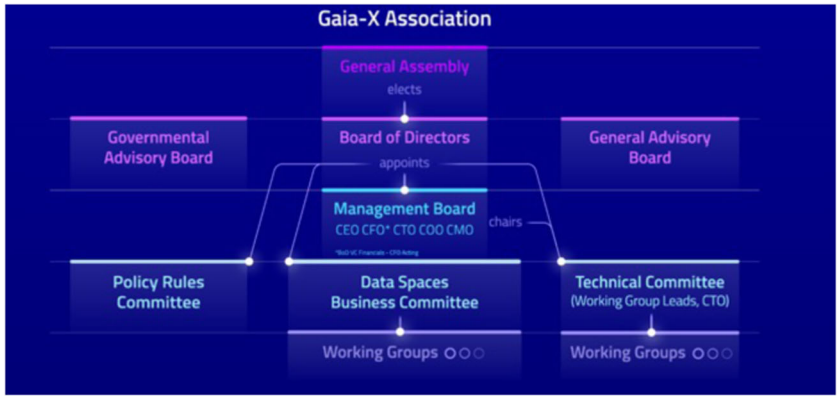

FIGURE 2 Gaia-X organisational structure. *Source*: Gaia-X.

To boost interoperability and portability, Gaia-X publishes policy rules and technical architecture rules, which are periodically updated. Policy rules represent the basis of compliance with the Gaia-X framework. They define the high-level principles to which companies adhering to Gaia-X need to abide in terms of cybersecurity, data protection, location of their service, switching and data portability (Gaia-X, 2020b). Architecture of standards (AoS), instead, define the list of technical and regulatory standards which are relevant for Gaia-X objectives, including open application programming interfaces (APIs) to enable data sharing, portability, and interoperability (Gaia-X, 2020b). In addition, the organisation develops open-source software code, common stacks, and labels to provide general guidance and increase trust by defining standards for data protection and immunity from non-European access. In other words, the plan is for European companies to 'scale through federation'(Bonfiglio, 2021, p. 9). Gaia-X's output is organized around ecosystems, or independent groups of companies and service providers that leverage the organisation's technical architecture to deliver solutions in specific sectors. Examples of ecosystems include Catena-X and Agdatahub, two projects for the circulation of data respectively in the automotive and agricultural sector, in line with EU data sovereignty rules (Gaia-X, 2022).

The European alliance for industrial data, edge, and cloud

A parallel initiative to Gaia-X is the European alliance for industrial data, edge and cloud. Announced by the European Commission in December 2021, it aims to 'strengthen the position of EU industry on cloud and edge technologies and capacities' (European Commission, 2021a). Unlike Gaia-X, which focuses on a federated technology by promoting open source code, interoperability between ecosystems, and common data spaces, the Alliance's work is more markedly premised on the need to support the competitiveness of European cloud solutions. The Terms of Reference of the Alliance explicitly refer to the fact that 'when European businesses currently use cloud services, they have little choice but to purchase services offered by non-European entities […] this can bring risks in terms of cybersecurity, supply vulnerabilities, switching possibilities as well as unlawful access to data by third countries' (European Commission, 2021c). By the same token, 'Participation in the Alliance should also serve to assist emerging providers of cloud services to overcome difficulties to scale-up at the European and global level, to reach sufficient scale to deliver services and compete effectively in the market' (European Commission, 2021c, p. 2). In practice, the Alliance is a forum for coordinating and unlocking investments in the strategic areas of cloud and edge computing. It is part of a series of industrial alliances supported by the EU Industrial Strategy to accelerate European competitiveness in strategic areas that would not develop through market processes only. The Alliance is also meant to better coordinate EU Member States' investments under the Important Projects of Common European Interest (IPCEIs).[9] The works of the Alliance are organized around two working groups; an Industrial Edge & Cloud working group composed of industry representatives, and an informal Member States Cloud Cooperation Group.

Two factors highlight the difference between Gaia-X and the Alliance: leadership and membership. With regard to leadership, Gaia-X is a private-led initiative with a focus on technical requirements and standards, while the Alliance can be considered more markedly political. The Alliance was launched by the European Commission and endorsed by EU Member States in the Declaration on European Cloud. As such, its works are facilitated by the Commission's Directorate-General for Communications Networks, Content and Technology (CNECT), which operates under the leadership of the Commissioner for the Internal Market. Regarding membership, while Gaia-X's works are shaped by both European and non-European members, the Alliance is currently open to European companies only. Its

Declaration states that membership of the Alliance is open to all companies whose activities can help establish a competitive European cloud ecosystem and meet the eligibility criteria (European Commission, 2021a). While in theory foreign companies can join the Alliance—provided they have a legal representative established in the Union (European Commission, 2021c)—in practice, the current list of members does not feature any non-European company (European Commission, 2022).

Analysis

As shown above, the structure of Gaia-X and the European Alliance on Industrial Data, Edge, and Cloud reflect two distinct approaches to industrial policy. Gaia-X is an 'open', industry-led initiative with a more inclusive approach to data sovereignty based on participants' individual input and technical expertise, regardless of their origin. By contrast, the Industrial Alliance is a more exclusive initiative with a stronger emphasis on European membership.

The distinctiveness of these organisations' approaches is reflected in their architecture. As detailed by its Chief Technology Officer (CTO), the objective of Gaia-X is to achieve data sovereignty by reversing the traditional 'code is law' paradigm (Lessig, 2000)—where the technology (code) determines the boundaries of what is possible and achievable—with the alternative 'law is code' or 'compliance as code' (Gronlier, 2022). This new paradigm reflects the idea that, instead of regulations and other compliance instruments catching up with technology, it is the technology itself that can be designed to ensure compliance with existing regulatory regimes (see World Economic Forum [WEF], 2022). In other words, the technology protocols and labels that form Gaia-X's trust framework should enable a form of 'automated compliance', which ensures that compliance with EU data sovereignty requirements is embedded in the use of Gaia-X's technology stack.

In the Alliance, instead, the focus is on a more traditional approach to industrial policy and innovation, namely on unlocking and coordinating investments on cloud and edge technologies coming from dedicated EU funding and the relevant IPCEI. In addition to that, the Alliance is in charge of establishing a dialogue between the Commission and the member states about their public sector strategies for the procurement of cloud services.

An analysis of the trajectories of these initiatives allows to observe that both approaches are facing unique challenges. With regard to Gaia-X, the inclusion of non-EU providers, are said to have become a hindrance to its objective of reducing European dependence on foreign cloud providers. The rationale for Gaia-X to include hyperscalers is to enable a multitiered infrastructure where data can be stored according to their criticality. Thus, noncritical data can still be stored in non-EU servers. Such approach theoretically allows for greater modularity in data storage while still benefitting from the scale provided by non-EU companies. In practice, however, the presence of non-EU CSPs may be seen as too contentious under current conditions. Declarations by officials involved in the works of Gaia-X suggest that the presence of American players, coupled with a lack of coordination and vision, might have contributed to create an excessive and unmanageable workload for the organisation (Goujard & Cerulus, 2021). With regard to bolstering the competitiveness of European cloud players, it seems that hyperscalers have a great influence in working groups where portability rules are discussed, thereby potentially undermining the possibility to enhance competitiveness in the European cloud sector (Goujard & Cerulus, 2021).

The issue of whether Gaia-X can achieve its objectives is reinforced by the withdrawal of one of its founders, French cloud provider Scaleway, from its works. An official communication by the company points at the negative impact of non-European cloud providers as the main reason for the withdrawal:

> Once they joined the technical committees, these dominant entities and their 'tech diplomats' flooded other contributors with orientations, requirement proposals and comments that, individually or collectively, the European collective could not possibly cope with, thereby introducing structural bias in the standard-like elaboration process. The risk being, therefore, to create standards favourable to the already dominant players, and not echoing the needs, expectations and challenges of the diverse local technology suppliers throughout Europe. (Scaleway, 2021)

According to the same company, non-EU CSPs are largely responsible for watering down the wording used to introduce security labels, for example by excluding the notion of 'extraterritoriality' from being mentioned in the strictest level of cybersecurity label published by Gaia-X (Scaleway, 2021). Echoing such concerns, the CEO of French cloud company OVH stated that non-European companies that are part of Gaia-X should seriously abide by its rules and values, or else be expelled (Goujard, 2021). Such comments about the allegedly dysfunctional setup of Gaia-X all point to the concern that non-EU CSPs might leverage the initiative as a 'trojan horse' to keep their dominance in the European cloud market by influencing its standards and technical specifications (Autolitano & Pawlowska, 2021).

Moreover, Gaia-X emphasis on inclusivity and participation is not always shared by all members. French cloud provider Clever Cloud, for instance, criticised declarations by Gaia-X that the CLOUD Act should not prompt excessive fear in Europeans, given the safeguards contained in the Act and the GDPR, and that Gaia-X could be 'the bridge between the CLOUD Act and the GDPR' (Westendarp & O'Brien, 2022). In this regard, however, it is worth considering that episodes of overt criticism against the inclusive set-up of Gaia-X so far have come mainly from French companies. As such, their views could be reasonably seen as expression of the more intransigent industrial policy approach adopted by the French government against the primacy of Big Tech companies.

Trade associations have also been accused of purposefully slowing down the works of Gaia-X's working groups by engaging in intense lobbying efforts to pass or block proposals. In this regard, the Secretary-General of the Cloud Infrastructure Service Providers in Europe (CISPE)—a European trade association that also represents AWS—suggested that trade associations should only have observer status and no voting rights in the working groups. CISPE also observed that Bitkom and DigitalEurope—two trade associations which also represent Microsoft, Google, and Amazon—are 'only providing lobbying services [which add] no value to our technical working group' (Westendarp & O'Brien, 2022). Views expressed by the industry, however, do not necessarily reflect those of the European Commission, whose Directorate-General for Competition has addressed a letter to Gaia-X's leadership, which clarifies that the organisation's membership does not seem to produce anticompetitive effects in its working groups (European Commission, 2021d).

Ultimately, the potential shortcomings that an initiative like Gaia-X faces can be seen as the inevitable by-product of its unique setup. Unlike traditional cloud service providers, the organisation is not a company with unified leadership, but rather a forum which needs to bring on board many companies with different sizes, origin, and objectives to produce its policy output. Moreover, there is a fundamental dissonance between Gaia-X's federative ambitions and the reality of the EU Digital Single Market, which is still fragmented along national market lines. This makes it more difficult for the association to pool resources and ensure participation from all relevant companies in the EU. In this regard, Gaia-X's national hubs, which are not a body of the association but act as central contact points for interested parties in each country, should help Gaia-X have a broader reach on European soil, as well as helping translate Gaia-X's offer in concrete use cases for each country. Yet while the

association has published several sector-specific use cases, at the time of writing these have only been launched in seven countries, without the widespread adoption needed to achieve a fully pan-European cloud ecosystem.

With regard to the European Alliance for Industrial Data, Edge, and Cloud, its focus on European membership seemingly shield it from the challenges that have beset Gaia-X since its inception. But the Alliance's activities have not been devoid of criticism. Since it was announced by the European Commission, questions have been raised about the potential risk of duplicating the work of Gaia-X and hence adding an unnecessary layer to the EU industrial policy efforts on cloud computing. In a panel dedicated to the presentation of the initiative, a Deputy Director of DG-CNECT clarified that this would not be the case. On the contrary, the Alliance would act like a bridge between Gaia-X and the Commission's priorities. In this regard, while Gaia-X would focus more squarely on technical standards and concrete user needs, as well as fostering cloud migration among European SMEs, the Alliance would channel strategic investments to ensure wide adoption of those technical standards at the European level (European Internet Forum [EIF], 2021). Such remarks echo Commissioner Breton's earlier declarations about the importance for the EU to establish synergies between the Alliance and Gaia-X as key contributors to its data sovereignty ambitions (Breton, 2020). However, in a response to a parliamentary question enquiring about the European Commission's alleged erratic stance on Gaia-X, the Commissioner for the Internal Market replied by stressing the role of Alliance in the Commission's cloud strategy, without mentioning Gaia-X (Veld, 2021). Finally, while the works of the Alliance have been going forward through bi-weekly meetings of its working groups, it remains to be seen whether the organisation will manage to effectively create synergies for strategic investment in EU cloud and edge capabilities.

CONCLUSION

This paper has analysed the strategic dimension of cloud computing with a focus on the European Union. In a geopolitical environment where digital technologies are crucial to wield influence, harnessing the potential of the data economy and its underlying infrastructure has become a priority among many polities. While the United States and China can count on cloud hyperscalers that enjoy sizable market shares at home and abroad, European member states are trailing in the development of their cloud capabilities. Consequently, EU governments find themselves in the predicament of balancing the strategic objective of migrating their data to the cloud with the need to reduce their dependence on foreign CSPs.

Against this backdrop, this article has shown how the EU is relying on its data sovereignty agenda to offset the lack of competitiveness of its cloud ecosystem. While addressing legitimate security concerns, data sovereignty provisions also serve the purpose of creating a regulatory space for European investments to flow and local companies to become more competitive in the cloud sector.

To illustrate the impact of data sovereignty on the EU industrial policy landscape, the paper has presented two case studies: Gaia-X and the European Alliance on Industrial Data, Edge, and Cloud. These initiatives reflect two distinct approaches to industrial policy. Gaia-X is an industry-led initiative to achieve scale, enhance interoperability, and enforce data sovereignty with a focus on technology, including standards and open-source code. By contrast, the Industrial Alliance is a Commission-led initiative with an emphasis on unlocking investments to achieve breakthroughs in cloud and edge computing. To gauge the efficacy of such policy initiatives in delivering the EU's targets of reducing its dependence on foreign CSPs and ensuring better safeguards for European data is beyond the scope of this paper. This study has shown, however, that while different in their setup both organisations face

obstacles to the achievement of their policy objectives. This is primarily due to the challenge of achieving results at a European scale while grappling with the reality of a Digital Single Market fragmented along national lines. In light of this, tracing the trajectory of such initiatives can provide insights into the future direction of the European industrial policy with a focus on data and the cloud.

The European data sovereignty agenda, embodied in the case studies mentioned above, can inspire polarising views. On the one hand, it could be seen as a mere attempt by European 'laggards' to catch up in a sector prone to consolidation and where European companies are fundamentally latecomers. In this view, data sovereignty could be dismissed as an industrial policy dressed up as competition policy, an attempt to erect barriers against foreign competitors while subsidising local players. On the other hand, some might praise data sovereignty as a genuine concern by a polity with high standards of data protection, which ensures interoperability and compliance with a range of safeguards in the cloud sector. More probably, the European posture is an attempt to square a principled approach to the governance of data with the realist view that European governments must develop a competitive cloud sector if they are to avoid sinking into strategic irrelevance.

ACKNOWLEDGEMENTS

The author wishes to thank Prof. Madeline Carr and three anonymous reviewers for helpful comments on an earlier version of this paper. Support from the Engineering and Physical Sciences Research Council (grant number EP/S022503/1) is gratefully acknowledged.

CONFLICT OF INTEREST STATEMENT

The author declares no conflict of interest.

DATA AVAILABILITY STATEMENT

No new datasets were generated or analysed during the current study. Market data supporting the findings of this study are cited in the list of references and are publicly available.

ORCID

Filippo Gualtiero Blancato https://orcid.org/0000-0003-4624-867X

ENDNOTES

[1] It should be noted, however, that the standard approach to security in the cloud is that of a 'share responsibility model', whereby both the vendor and the customer are responsible for the security of data in the cloud, with a degree that varies depending on the cloud service and deployment (see Section "The strategic dimension of the cloud: a brief overview").

[2] For a full list of primary sources, see Supporting Information: Appendix II.

[3] In cloud computing, hyperscalers are those vendors whose extensive network of data centres across various regions allows them to offer computing and storage services at scale. Among western companies, the expression is used to refer mainly, but not exclusively, to companies such as Amazon Web Services, Microsoft Azure, and Google Cloud.

[4] Other countries outside the EU have expressed similar concerns around the state of the cloud market. For example, the UK the Office of Communications (Ofcom) has published an interim report on cloud services highlighting that features such as egress fees, technical restrictions on interoperability and committed spend discounts can make it more difficult to switch between providers and further entrench the dominant position of incumbents (See Ofcom, 2023).

[5] At the time of writing, the ACM is the only European authority to have published a comprehensive, in-depth study of the cloud computing market.

[6] Figures refer to all cloud layers combined, with the exception of productivity software. ACM clarifies that 'the market share of Azure may be underestimated, because part of Microsoft's SaaS services are probably not included in the revenue figures supplied to ACM' (p. 34, footnote 83).

[7] The range of HHI takes into account the range of market shares provided in Table 1.

[8] Western Europe includes: AT, BE, DK, FI, FR, DE, EL, EI, IT, NL, PO, ES, SE plus CH, NO, UK.

[9] IPCEIs are cross-border projects which allow Member States to invest jointly in strategic areas to enable breakthrough innovation in key technologies for the European economy. In essence, they are exemptions to state aid rules, which would normally forbid subsidisation of chosen sectors by Member States. At present, EU Member States have proposed IPCEIs in a number of technologies, including cloud computing through the IPCEI on Next Generation Cloud Infrastructure and Services (IPCEI-CIS) (European Commission, 2021b).

REFERENCES

Abraha, H. H. (2020). Regulating law enforcement access to electronic evidence across borders: The United States approach. *Information & Communications Technology Law*, *29*(3), 324–353. https://doi.org/10.1080/13600834.2020.1794617

ACN. (2021). *Strategia cloud Italia. Ministro per l'innovazione tecnologica e la transizione digitale*. https://innovazione.gov.it/dipartimento/focus/strategia-cloud-italia/

Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access*, *9*, 57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203

Authority for Consumers & Markets (ACM). (2022). *Market study into cloud services*. https://www.acm.nl/en/publications/market-study-cloud-services

Autolitano, S., & Pawlowska, A. (2021). *Europe's quest for digital sovereignty: GAIA-X as a case study*. Istituto Affari Internazionali, IAI Papers 21. https://www.iai.it/en/pubblicazioni/europes-quest-digital-sovereignty-gaia-x-case-study

Bayart, B., & Martin, J. O. (2018). *Thierry Breton: 'C'est aux Gafa de s'adapter à nos règles, pas l'inverse'*. Le Figaro. https://www.lefigaro.fr/secteur/high-tech/2018/04/06/32001-20180406ARTFIG

Bmwk. (2019). *Press release on Franco-German common work on a secure and trustworthy data infrastructure*. https://www.bmwk.de/Redaktion/EN/Pressemitteilungen/2019/20191029-press-release-on-franco-german-common-work-on-a-secure-and-trustworthy-data-infrastructure.html

Bonfiglio, F. (2021). *Gaia-X vision and strategy*. https://gaia-x.eu/wp-content/uploads/2021/12/Vision-Strategy.pdf

Breton, T. (2020). *We have one chance to bring Europe to the top of the race in the data economy but we have to act jointly & fast*. Together with the future Alliance on Industrial Data and Cloud, we see GaiaX as a key contributor to achieve our ambition. https://twitter.com/thierrybreton/status/1329072397043916802?lang=en-GB

Brier, T. F. (2017). Defining the limits of governmental access to personal data stored in the cloud: An analysis and critique of Microsoft Ireland. *Journal of Information Policy*, *7*, 327–371. https://doi.org/10.5325/jinfopoli.7.2017.0327

BSA. (2021). *The CLOUD act and the European Union: Myths vs facts*. https://www.bsa.org/files/policy-filings/02282019CLOUDACTEUMythvsFact.pdf

BSI. (2020). *Cloud computing compliance criteria catalogue*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CloudComputing/ComplianceControlsCatalogue/2020/C5_2020.pdf?__blob=publicationFile&v=3

Byrne, D., Corrado, C., & Sichel, D. (2018). *The rise of cloud computing: Minding your P's, Q's and K's*. National Bureau of Economic Research, Working Paper. https://doi.org/10.3386/w25188

Carr, N. G. (2008). *The big switch: Rewiring the world, from Edison to Google* (1st ed). W. W. Norton & Co.

Council of the EU. (2023 Juanuary 25). *Electronic evidence: Council confirms agreement with the European parliament on new rules to improve cross-border access to e-evidence* [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/

Coyle, D. (2021). *Cogs and monsters. What economics is, and what it should be*. Princeton University Press.

Daskal, J. (2015). The un-territoriality of data. *Yale Law Journal*, *125*, 326–398.

Data Act. (2022). *Official text*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN

Digital Markets Act. (2020). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN

ENISA. (2011). *Security and resilience in governmental clouds*. ENISA Report. https://www.enisa.europa.eu/publications/security-and-resilience-in-governmental-clouds

European Commission. (2004). Guidelines on the assessment of horizontal mergers under the council regulation on the control of concentrations between undertakings. *Official Journal of the European Union*. https://eur-lex.

europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52004XC0205(02)&from=EN#:~:text=In%20order%20to%20measure%20concentration,in%20the%20market%20(18)

European Commission. (2018). *Regulation on European Production and Preservation Orders for electronic evidence in criminal matters*. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225#:~:text=The%20European%20Production%20Order%20and,proceedings%20for%20concrete%20criminal%20offences

European Commission. (2019). *European commission cloud strategy*. https://ec.europa.eu/info/publications/european-commission-cloud-strategy_en

European Commission. (2020a). *Advanced technologies for industry—At watch*. Technology Focus on Cloud Computing. https://ati.ec.europa.eu/news/technology-watch-cloud-computing

European Commission. (2020b). *A European strategy for data*. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066

European Commission. (2021a). *Declaration of the European alliance for industrial data, edge and cloud*. https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance#:~:text=The%20European%20Alliance%20for%20Industrial,States%20representatives%20and%20relevant%20experts

European Commission. (2021b). *Strategic dependencies and capacities*. Staff Working Document Accompanying the 2020 New Industrial Strategy. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021SC0352&from=en

European Commission. (2021c). *State aid: Commission adopts revised State aid rules*. Press release. https://ec.europa.eu/commission/presscorner/detail/en/IP_21_6245

European Commission. (2021d). *EU strategic dependencies and capacities: Second stage of in-depth reviews*. https://ec.europa.eu/docsroom/documents/48878

European Commission. (2022). *Commission implementing decision on the adequate level of protection of personal data under EU-US data privacy framework*. https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf

European Industrial Technology Roadmap. (2021). https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf

European Internet Forum (EIF). (2021). *The European alliance for industrial data and cloud—Panel discussion—Full recording*. https://www.youtube.com/watch?v=guc7OEdii6A

Falknerath, R., & Rosenzweig, P. (2012). *Op-ed: Encryption, not restriction, is the key to safe cloud computing*. https://www.nextgov.com/it-modernization/2012/10/op-ed-encryption-not-restriction-key-safe-cloud-computing/58608/

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

Forrester. (2022). *The state of the cloud in North America, 2022: Modernization and cloud native will be the new normal*. https://www.forrester.com/press-newsroom/the-state-of-cloud-in-north-america-2022/#:~:text=Key%20findings%3A,%25%20of%20infrastructure%20decision%2Dmakers

Fox-Martin, A. (2022). *Advancing digital sovereignty on Europe's terms*. Google Cloud Blog. https://cloud.google.com/blog/products/identity-security/advancing-digital-sovereignty-on-europes-terms

Gaia-X. (2020a). *GAIA-X: A pitch towards Europe*. https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-a-pitch-towards-europe.pdf?__blob=publicationFile&v=6

Gaia-X. (2020b). *GAIA-X: Policy rules and architecture of standards*. https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-policy-rules-and-architecture-of-standards.pdf?__blob=publicationFile&v=3

Gaia-X. (2021). *Gaia-X members' list*. https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Downloads/gaia-press-release-march-31-list-en.pdf?__blob=publicationFile&v=3

Gaia-X. (2022). *Gaia-X architecture document*. https://docs.gaia-x.eu/technical-committee/architecture-document/22.10/

Garman, M. (2022). *AWS digital sovereignty pledge: Control without compromise*. AWS Security Blog. https://aws.amazon.com/blogs/security/aws-digital-sovereignty-pledge-control-without-compromise/

Gartner. (2022). *Gartner forecasts worldwide public cloud end-user spending to reach nearly $500 billion in 2022*. https://www.gartner.com/en/newsroom/press-releases/2022-04-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-nearly-500-billion-in-2022

Geradin, D., Bania, K., Katsifis, D., & Circiumaru, A. (2022). *The regulation of cloud computing: Getting it right*. https://doi.org/10.2139/ssrn.4285731

Gleeson, N., & Walden, I. (2021). Facilitating competition in the cloud. In C. Millard (Ed.), *Cloud computing law* (2nd ed, pp. 477–500). Oxford University Press.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford University Press.

Goujard, C. (2021). *French cloud firm warns Microsoft, Alibaba to 'respect' Gaia-X rules*. https://pro.politico.eu/news/143447

Goujard, C., & Cerulus, L. (2021). *Inside Gaia-X: How chaos and infighting are killing Europe's grand cloud project*. Politico. https://www.politico.eu/article/chaos-and-infighting-are-killing-europes-grand-cloud-project/

Gronlier, P. (2022). *Compliance as code*. Gaia-X Blog. https://gaia-x.eu/news/latest-news/gaia-x-compliance-as-code/

Helpman, E. (1998). *General Purpose Technologies and Economic Growth*. MIT Press.

Herr, T. (2020a). *Better to be realistic about the security opportunities of cloud computing*. Lawfare Blog. https://www.lawfareblog.com/better-be-realistic-about-security-opportunities-cloud-computing

Herr, T. (2020b). *Four myths about the cloud: The geopolitics of cloud computing*. Report, Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/four-myths-about-the-cloud-the-geopolitics-of-cloud-computing/

Hon, W. K., Millard, C., Singh, J., Walden, I., & Crowcroft, J. (2016). Policy, legal and regulatory implications of a Europe-only cloud. *International Journal of Law and Information Technology*, *24*(3), 251–278. https://doi.org/10.1093/ijlit/eaw006

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 1–15. https://doi.org/10.1177/2053951720982012

Ionos. (2019). *The controversial cloud act*. https://cloud.ionos.co.uk/white-paper/cloud-act

Irion, K. (2012). Government cloud computing and national data sovereignty. *Policy & Internet*, *4*(3–4), 40–71. https://doi.org/10.1002/poi3.10

Joint Declaration on Cloud. (2020). *Towards a next generation cloud for Europe*. https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

Krasner, S. D. (1988). Sovereignty. *Comparative Political Studies*. *21*(1), 66–94. https://doi.org/10.1177/0010414088021001004

Kushida, K. E., Murray, J., & Zysman, J. (2011). Diffusing the cloud: Cloud computing and implications for public policy. *Journal of Industry, Competition and Trade*, *11*(3), 209–237. https://doi.org/10.1007/s10842-011-0106-5

Kushida, K. E., Murray, J., & Zysman, J. (2015). Cloud computing: From scarcity to abundance. *Journal of Industry, Competition and Trade*, *15*(1), 5–19. https://doi.org/10.1007/s10842-014-0188-y

Lessig, L. (2000). *Code is law*. Harvard Magazine. https://www.harvardmagazine.com/2000/01/code-is-law-html

Lianos, I. (2019). *The future of competition policy in Europe. Some reflections on the interaction between industrial policy and competition law*. CLES Policy Paper, Faculty of Laws. https://www.ucl.ac.uk/cles/sites/cles/files/cles_policy_paper_1_2019.pdf

Lundqvist, B. (2019). Cloud services as the ultimate (gate)keeper. *Journal of Antitrust Enforcement*, *7*(7), 220–248. https://doi.org/10.1093/jaenfo/jny013

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing*. https://csrc.nist.gov/publications/detail/sp/800-145/final

Mueller, M. (2017). *Will the Internet fragment? Sovereignty, globalization, and cyberspace*. Polity Press.

Mueller, M. L., & Farhat, K. (2022). Regulation of platform market access by the United States and China: Neo-mercantilism in digital services. *Policy & Internet*, *14*(2), 348–367. https://doi.org/10.1002/poi3.305

OVHCloud. (2021). *The European cloud industry: A market worth €300bn+ by 2027-2030. Could half of this potential growth slip through Europe's hands?* https://corporate.ovhcloud.com/en-gb/newsroom/news/europe-cloud-challenges-key-and-five-scenarios-impact/

Pavic, I., Galetic, F., & Piplica, D. (2016). Similarities and differences between the CR and HHI as an indicator of market concentration and market power. *British Journal of Economics, Management & Trade*, *13*(1), 1–8. https://doi.org/10.9734/BJEMT/2016/23193

Propp, K. (2019). *Waving the flag of digital sovereignty*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/waving-the-flag-of-digital-sovereignty/

Propp, K. (2022). *European cybersecurity regulation takes a sovereign turn*. European Law Blog. https://europeanlawblog.eu/2022/09/12/european-cybersecurity-regulation-takes-a-sovereign-turn/

Rapport n° 7 Sénat. (2019). *Le devoir de souveraineté numérique*. http://www.senat.fr/rap/r19-007-1/r19-007-1.html

Renda, A. (2022). *The data act: Six impossible things before breakfst?* https://www.ceps.eu/the-data-act-six-impossible-things-before-breakfast/

Sanders, C. (2022). *Microsoft cloud for sovereignty: The most flexible and comprehensive solution for digital sovereignty*. Microsoft Blog. https://blogs.microsoft.com/blog/2022/07/19/microsoft-cloud-for-sovereignty-the-most-flexible-and-comprehensive-solution-for-digital-sovereignty/

Scaleway. (2021). *Full steam ahead towards a true multi-cloud offering to deliver on broken promises*. Scaleway Blog. https://blog.scaleway.com/full-steam-ahead-towards-a-true-multi-cloud-offering-to-deliver-on-broken-promises/

Schneier, B. (2019). *We have root: Even more advice from Schneier on security*. Wiley.

Schwartz, P. M. (2018). Legal access to the global cloud. *Columbia Law Review*, *118*(6), 1681–1762. https://www.jstor.org/stable/26511248

Smith. (2021). *Answering Europe's call: Storing and processing EU data in the EU*. EU Policy Blog. https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/

Stratégie Nationale Cloud: Lancement du Plan Industriel de Soutien à la Filière. (2021). https://www.entreprises.gouv.fr/fr/actualites/numerique/strategie-nationale-cloud-lancement-du-plan-industriel-de-soutien-la-filiere

Stupp. (2022). *European cloud restrictions could limit U.S. providers' reach*. Wall Street Journal. https://www.wsj.com/articles/european-cloud-restrictions-could-limit-u-s-providers-reach-11656430248?mod=article_inline

Synergy Group. (2020). *Amazon and Microsoft lead the cloud in all major European countries*. https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries

Synergy Group. (2021b). *Huge cloud market still growing at 34% per year; Amazon, Microsoft & Google now account for 65% of the total*. https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues

Synergy Group. (2022). *European cloud providers continue to grow but still lose market share*. https://www.srgresearch.com/articles/european-cloud-providers-continue-to-grow-but-still-lose-market-share

Veld, S. I. 'T. (2021). *Parliamentary question. The Commission's strategy towards GaiaX, an initiative sponsored by Chinese companies* | E-005217/2021 | European Parliament. https://www.europarl.europa.eu/doceo/document/E-9-2021-005217_EN.html

Wang, S., & Casado, M. (2021). The cost of cloud, a trillion dollar paradox. *Andreessen Horowitz*, 1–11. https://a16z.com/2021/05/27/cost-of-cloud-paradox-market-cap-cloud-lifecycle-scale-growth-repatriation-optimization/

Westendardp, L., & O'Brien, P. (2022). *Gaia-X board member blames lobbying for project's gridlock*. Politico PRO. https://pro.politico.eu/news/152350

World Economic Forum. (2022). *Regulatory technology for the 21st century*. White Paper. https://www.weforum.org/whitepapers/regulatory-technology-for-the-21st-century/

SUPPORTING INFORMATION

Additional supporting information can be found online in the Supporting Information section at the end of this article.

How to cite this article: Blancato, F. G. (2023). The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*, 1–21. https://doi.org/10.1002/poi3.358