The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X

Adler-Nissen, Rebecca; Eggeling, Kristin Anabel

Published in:
Journal of Common Market Studies

Publication date:
2024

Document license:
Other

Citation for published version (APA):
Abstract

This article explores the struggle for ‘digital sovereignty’ in the European Union. A seeming contradiction – the internet, after all, spans the globe – digital sovereignty is portrayed as the winning geo-economic formula to keep the EU secure, competitive, and democratic in the digital future. Approaching digital sovereignty as a discursive claim and analysing it through a case study of the European cloud project Gaia-X, we show that there is no singular understanding of digital sovereignty in the EU. Instead, we identify six different conceptions across the domains of security, economy and rights. The article outlines three scenarios for how the digital sovereignty agenda may develop and thus shape the EU’s digital policy and its relations with the rest of the world: constitutional tolerance (where the conceptions co-exist), hegemony (where one conception dominates), or collapse (where the agenda falls apart due to inbuilt conceptual contradictions).

Keywords: Cloud; Cybersecurity; Data; Digital Sovereignty; Geopolitics; Rights
Introduction

In the mid 2020s, we live in a ‘technopolar’ era where big tech companies are challenging the status of the state (Bremmer, 2021). The EU only recently began to respond to these developments by calling for ‘digital sovereignty’. A slippery term, ‘digital sovereignty’ is not only portrayed as an attempt to catch up, but also as a ‘third way’ alternative to US surveillance capitalism and Chinese and Russian techno-authoritarianism committed instead to European norms and values (Giddens 2020). This article focuses on how the EU responds to geopolitical pressures by claiming sovereignty in the digital sphere and contributes to the debate about technology as an area of political contestation in Europe.

So far, most research has tried to clarify what digital sovereignty means (Pohle and Thiel, 2020), but few explore the political implications of its competing meanings and how this shapes the EU’s power (Broeders, Cristiano, and Kaminska, 2023). To contribute to the latter discussion, we suggest treating digital sovereignty as a discursive claim and follow scholarship that has called discursive ambiguity a feature of the concept, not a bug that can be resolved by fixing a final definition (Lambach and Oppermann, 2022). Specifically, we ask what happens when the two unstable and loaded terms ‘digital’ and ‘sovereignty’ meet and are put forward as a (geo)political agenda for Europe?

Our analysis demonstrates that while different actors publically embrace digital sovereignty, they do not share a singular understanding of the term, but push fundamentally different conceptions. This ambiguity, we argue, is crucial for its politics and effects.
Specifically, different conceptions of digital sovereignty give rise to different ideas about the EU, its digital single market and place in the world. We explore how these conceptions may shape not only the EU’s digital agenda but also the relation between ‘geopoliticization’ and digitalization.

We make sense of this through a case study of Gaia-X, Europe’s first and most prominent collective cloud project. According to its public and official representations, Gaia-X combines ‘digital’ and ‘sovereignty’ in multiple and enigmatic ways. First, it is expected to provide security through ‘secure data infrastructure’ by preventing overreliance on foreign providers. Second, it is to contribute to growth and ‘[i]nnovation’ by advancing the European cloud market and transforming it from a playground for foreign tech giants into a place for ‘European champions’ (French President Macron cited in Gartner, 2019). Third, it will promote European rights and values, such as the self-determination of users to operate their own technology choices.

In the sections below, we take a closer look at the official discourses surrounding the Gaia-X project and identify and analyze six comparatively distinct and individually ambiguous conceptions of digital sovereignty attached to Gaia-X across the security, economy and rights domains. As security, digital sovereignty is meant to either protect Europe from the outside through data localization or enable foreign tech giants

---

2 See Herranz-Surrallés, Damro and Eckert (2024) for a definition of ‘geopoliticization’.
4 See: https://www.gaia-x.eu/what-is-gaia-x.
5 The European cloud market is expected to grow by more than 25 per cent growth per year. At the moment, 70 per cent of this market is dominated by US providers, with the biggest European provider, Deutsche Telekom, serving a mere 2 per cent of the market. See: https://www.dw.com/en/gaia-x-cloud-a-safe-haven-for-europes-data/a-59724779.
6 This conceptual division resembles Lambach and Opperman’s (2022) article on digital sovereignty discourses in Germany. One key difference is our focus on territoriality and geoecnomics.
and countries to protect European security. In the economic domain, Gaia-X will either empower European tech champions or boost innovation by increasing trade and competition with the rest of the world. Finally, for the rights domain, citizens and collectives are either the holders of unsharable data sovereignty or empowered to choose how to share their data with the rest of the world. The article discusses how the six conceptions relate and produce different spaces of political thought and action — that could result in either constitutional pluralism, hegemony, or collapse. We conclude by discussing how these relations shape Europe’s self-understanding, digital market and role in the world.

Theory: ‘Digital sovereignty’ as performative discourse

Theoretically, we follow a poststructural understanding of discourse, highlighting the contingency and instability of language and meaning (Hansen, 2006). Whereas framing theory focuses on justifications of a particular policy (Damro and Christou, 2024), we treat the competing conceptions of digital sovereignty not only as interpretive, but as productive of the world they describe or react to. Our approach thus foregrounds the performative nature of claiming digital sovereignty. Digital sovereignty, in other words, is a discourse constituted via claims, or speech-acts, about what it ‘is’, does and promises for Europe.

Adopting a performative approach is useful for studying a political agenda that introduces a classic, yet slippery, political concept – sovereignty – into a debate on
governing fast-changing technologies. While sovereignty may take different meanings, it also has a specificity: there is always a *constituting* power (who or what ‘makes’ sovereignty) and a *constituted* power (who or what 'becomes' sovereign) (Bartelson, 2006). We thus ask: Who (or what) will provide digital sovereignty, for whom (or what) and in what domain?

Many textbooks define sovereignty as the supreme authority over a political entity (a polity, typically a state) that holds a territory (James 1999). In this light, the EU’s claims to digital sovereignty are twice unsettling. First, unlike traditional territorial conceptions of political spaces, they are attached to cyberspace and the digital market (Kremer and Mueller, 2014; Lambach 2020). Legal scholars have long debated whether sovereignty is even possible in the digital realm and how it relates to territory. Some emphasize the necessity of a post-territorial notion of sovereignty (Tsa-gourias, 2015). Others insist that even though the digital sphere complicates issues of extraterritorial jurisdiction (Irion, 2012), it is (or should) still be possible for states to claim sovereignty. As Sarah Mainwaring writes, the idea that digital technology, including cloud computing, is somehow void of territoriality is strange given the infrastructure such as undersea cables underpinning it (Mainwaring, 2020). Political economists warn that ‘hard-line’ digital sovereignty approaches, looking to fragment cyberspace, will threaten the global economy (Mitchell and Samlidis, 2021). In this reading, digital sovereignty reduces economic efficiency by requiring physical

---

7 Conceptualisations of digital sovereignty (Couture and Toupin, 2019) overlap with neighbouring concepts such as ‘technological sovereignty’, ‘data sovereignty’, or ‘virtual sovereignty’. They all embrace notions of control, but their articulations are shaped by distinct histories, see also Bellanova, Carrapico, and Duez, 2022 for an overview.
localisation in computing infrastructure. This is why digital sovereignty claims inevitably bring up deeper questions of territoriality and in our case, how to envisage Europe as a (geo)political space and market (Obendiek, 2022, p. 11).

The second way that the EU’s claims to digital sovereignty are unsettling is that, unlike Russian or Chinese articulations, digital sovereignty in Europe is not claimed by the state, but by the EU or tech actors. China has long sought ‘technological sovereignty’ to replace foreign digital infrastructure with local ones, while Russia seeks ‘internet sovereignty’ (Hong and Goodnight, 2020). In both cases, the state claims sovereignty for itself and its people. In the EU, digital sovereignty is not necessarily constituted in member states or national populations, but in citizens, markets, companies, and even machines. In this sense, European digital sovereignty claims resonate with earlier times when sovereignty was constituted in private companies or individuals – kings, emperors, or citizens (Glasze et al., 2022; Mérand, 2021; Bellamy, 2003). In addition to territorial and representational ambiguity, competing economic demands endorse the protection of the digital single market, on the one hand, and technological innovation and global competitiveness, on the other. As we shall see, because digital sovereignty lacks stable referents, it promotes contradictory policies.

Case, methods and data

---

8 European-level digital sovereignty is ‘inevitably pitching supranational against intergovernmental outlooks’ (Lambach and Oppermann, 2022).
Given that the digital sovereignty agenda is so broad, we address it through a single illustrative case study. Our case comes from the field of cloud computing, a technology that has received heavy investments in recent years, comparable to AI and semiconductors. Within cloud computing, we focus on Gaia-X, the first and until today most prominent collective European cloud project. At first sight, talking about sovereignty in relation to cloud computing may seem odd. In practice, ‘the cloud’ means ‘on demand remote use of IT services’ (Baur, 2023, 2) that provides users with fast and flexible computing capacity and storage space. Most of us use cloud technology every day when we send emails, check bank accounts, or post on social media. Cloud users have limited control over where their data is stored and which jurisdictions govern it (Eichensehr, 2016). Since data is distributed widely in a cloud, some argue, ‘it does not make sense to think of data as something that occupies an identifiable territory at all’ (Vatanparast, 2020). Nevertheless, since data storage depends on material infrastructures, such as data servers, it does not make sense to refer to it as ‘non-territorial’ either. Therefore, scholars often refer to cloud computing as post-territorial.

Gaia-X was first announced in October 2019 at the German Digitalgipfel by the (then) German Minister of Economic Affairs, Peter Altmaier. It was around this time, too, that the idea of European digital sovereignty was beginning to make headlines in European newspapers. What we need, Altmaier (2019) said, is:

… something that resembles an Airbus of artificial intelligence… in this disruptive world, in which cards are dealt in new ways and planes for manoeuvre are redefined, we need to redefine our interests and pool our
resources… Gaia X, the project we are launching here today, will help us achieve this: we will no longer be users only, but also inventors and implementers.

Already in Altmaier’s launch statement we can detect contradictions. The mentioning of a company (Airbus) next to the ambiguous ‘we’ (Germany? Europe? Citizens?) that will come to define the Gaia-X project is revelatory of the competing discursive claims at the heart of Europe’s digital sovereignty agenda. Other prominent EU initiatives such as the Digital Service Act or Digital Markets Act have a similarly ambiguous character. However, Gaia-X is particularly instructive because it is a concrete project that showcases a dizzying range of discursive struggles over digital sovereignty across different domains, characteristic of the broader body of EU regulation of digital technology.

Our analysis of Gaia-X relies on two main data sources: official Gaia-X documents and agendas from 2019 to 2023, and press releases, speeches, and manifestos by national and EU leaders that mention ‘Gaia-X’ and ‘sovereignty’. Our research is necessarily partial. For example, interviews with relevant stake-holders would add more depth as well texts in other languages than English, German, Danish and French. However, our aim is neither to cover all events, nor to trace each position, but to develop an empirically informed theoretical understanding of the struggle for ‘digital sovereignty’ and its implications for the geoeconomic turn of the digital market. We analyse the text corpus using discourse analytical strategies, looking for dominant narratives, us-vs-them dichotomies, historications, and future projections.
Specifically, we focus on who or what constitutes sovereignty and who or what is constituted as sovereign and in which domain.

**Digital sovereignty and the geo-economic turn of the digital single market**

To understand where the idea of digital sovereignty, and the appeal of projects like Gaia-X comes from, it is helpful to turn the clocks back to 2013 when Edward Snowden revealed the global scale of digital surveillance. In Europe, the first reaction was a widespread loss of trust. As Nellie Kroes, (former) Vice President of the European Commission, put it: If European cloud customers cannot trust the United States government or their assurances, then maybe they won’t trust US cloud providers either (European Commission, 2013). Kroes continued: ‘[I]f I am right then there are multi-billion euro consequences for American companies. Privacy is not only a fundamental right, it can also be a competitive advantage’, warning US cloud providers that they may lose access to the European market. The Court of Justice also questioned the transfer of personal European data to the US, setting the tone for a European alternative (Baur, 2023, p. 4).

Until then, the EU’s policies on digital services had predominantly promoted liberalization and global trade. Allegedly, the EU was ‘falling behind’ other developed economies and access to content needed to be ‘opened up’. Therefore the EU sought to make online and cross-border trade ‘more straightforward’ (European Commission, 2010). The guiding principle was innovation- and business-friendly regulation in line with the ‘liberal order’ (Herranz-Surrallés, Damro and Eckert, 2024).
Gradually, throughout the second half of the 2010 and early 2020s, EU legislation became more restrictive as Snowden’s revelations were accompanied by new threats: abuse by dominant market leaders (Monti and Rangoni, 2022), fraud, and lack of responsibility for illegal content. This raised questions of how to ensure the protection of fundamental rights of citizens to privacy and security vis-à-vis other states and especially from private companies. The European response became increasingly driven by ‘politics of control’ (Mager, 2017) that led, most importantly, to the 2016 General Data Protection Regulation (GDPR). Anu Bradford’s (2020) *The Brussels Effect* documents how the EU became a normative standard setter with the GDPR by using its market power (Haroche 2024).

Yet, in contrast to GDPR, the emerging discourse of digital sovereignty is not merely focused on data or consumer protection rights, but a broader response to geoeconomic and technological developments. Calls for digital sovereignty emerged also as responses to cyber threats, Russian interference in electoral processes, an emerging US-Chinese tech-trade war as well as a growing reliance on foreign cloud infrastructure and the US as an increasingly unreliable partner (Bauerle-Danzmann and Meunier, 2024). In this climate, the EU’s Digital Agenda 2020-30 announced to ‘create secure digital spaces and services, and develop level playing fields in digital markets with large platforms and strengthen the EU’s digital sovereignty’ (European Parliament, 2022). The usual growth and innovation language is now accompanied by references to protection and autonomy.

*The making of Gaia-X*
Responding to a sense of increased vulnerability, several EU member states started developing their own cloud system in the 2010s. Germany worked on the ‘Trusted Cloud’ and the Bundescloud, the UK (then still an EU member state) sought to build a G-cloud, and France had Andromède, to mention a few. None of them were successful and Gaia-X is the European answer to these national projects. In the early stages, German Chancellor Angela Merkel imagined ‘European providers that offer security for our citizens, so that one shouldn’t have to send emails and other information across the Atlantic’.\(^9\) However, today we know that Gaia-X does not offer its own cloud services but is an ‘infrastructure’ or ‘ecosystem’ for data in Europe and beyond. If we think of single member state initiatives and the cloud products of commercial providers like Amazon or Microsoft as cars, Gaia-X is the road and traffic system they navigate. Yet, the dream to build an EU-wide cloud was complicated by bumps along the road.

After the project was announced in Germany, Altmaier’s Ministry suggested that it should be developed jointly with France (Altmaier, 2019).\(^{10}\) French political and business leaders officially got involved on February 18, 2020 (Federal Ministry for Economic Affairs and Energy, 2020a), exactly one day before the von der Leyen Commission’s publication of the European Data Strategy on February 19, 2020 (European Commission, 2020). In June 2020, Gaia-X received funding from Brussels. The project fits both into the digitalization-focused agenda of Germany’s Council Presidency in 2020, and the Commission’s narrative of data autonomy. This was underlined by von der Leyen’s State of the Union address in 2020: ‘A real data economy… would be a

---

powerful engine for innovation and new jobs... we need to secure this data for Europe and make it widely accessible.’

In June 2020, the Gaia-X Association was set up as a non-profit organisation under Belgian law (AISLB) and opened an office within walking distance from the European Commission. In November 2020, an EU-27 Joint Declaration hailed Gaia-X as an exemplary project, and in January 2021, the Commission founded the European Alliance for Industrial Data, Edge and Cloud tasked with developing the ‘EU Cloud Rulebook’ (European Commission, 2020). In March that year, von der Leyen labelled the 2020s ‘Europe’s digital decade’ (European Commission, 2021) and shortly after affirmed the critical geopolitical importance of cloud technology.

Contradictions emerge

In late 2021, reportedly, ‘the project was struggling to get off the ground amid infighting between corporate members, disagreement over its overall aims and a bloated bureaucratic structure’. Part of the problem was unclear administration, caught between the Brussels Foundation office, national Gaia-X hubs, surging memberships and simultaneous resignations of some of its founding members (Donelly, 2021). Another issue was the fact that non-European tech-companies joined Gaia-X working groups, among them the ‘dubious bedfellows’ – notably, Amazon,

---

Google and Microsoft. Gaia-X communication underlines that the presence of foreign data giants is based on common interests that outweigh differences. As the Chief Technology Officer at the Gaia-X Association, Boris Otto, said: ‘We don't want to isolate Europe, but seek to invite anyone who agrees to play by our rules’. The tech corporations, in turn, have a different understanding of how to help Europe in its quest for ‘digital sovereignty’. Microsoft, for instance, endorsed the project’s ‘open and market-driven approach’ and the opportunities it offers for value generation, pioneering business models, and innovations (Klynge, 2020). Below we offer a possible explanation for such and other internal tensions, drawing out the competing discourses in Gaia-X and the European digital sovereignty debate.

The following sections analyze this debate. We identify six competing discursive claims about digital sovereignty that are all politically salient, encouraging some policies while marginalizing others. Their implications reach far beyond tech policy and may shape debates on EU security politics, economic development, and individual rights for years to come. As we show, in each domain of digital sovereignty we can identify two distinct conceptions: one that is bounded, exclusive, and territorial, and another that is boundless and post-territorial (Table 1). This indicates that Gaia-X may in its current state be considered an example of ‘superficial geopoliticisation’, as its main effect has so far been the re-shaping of discursive politics rather than concrete policy practice.


17 Our territorial/post-territorial distinction should not be confounded with the defensive/offensive distinction discussed in Haroche (2024) and Bauerle-Danzmann and Meunier (2024).
Table 1: Six claims to digital sovereignty

<table>
<thead>
<tr>
<th>Domains</th>
<th>Security</th>
<th>Economy</th>
<th>Rights¹⁸</th>
</tr>
</thead>
<tbody>
<tr>
<td>Territorial</td>
<td>Strategic autonomy</td>
<td>Neo-mercantilism</td>
<td>Personal privacy</td>
</tr>
<tr>
<td>Post-territorial</td>
<td>Cybersecurity</td>
<td>Market cosmopolitanism</td>
<td>Data ownership</td>
</tr>
</tbody>
</table>

Digital sovereignty as security

In the security domain, Gaia-X is imagined to deliver digital sovereignty either by protecting Europe from the outside (by insisting on data localization and using EU-made infrastructure) or by enabling outsiders to protect European security (reflected in the paradoxical situation that foreign tech giants are members of Gaia-X).

Strategic autonomy

¹⁸ The dotted line in ‘Rights’ domain signals an even less clear distinction between territorial and post-territorial than in the other two domains.
When digital sovereignty is understood as ‘strategic autonomy’ in the context of Gaia-X, the idea is that Europe has to free itself from its reliance on foreign cloud infrastructures. The dependence on foreign providers brings control from other countries, which play by different rules concerning privacy and government access to data. At the same time, member states and the EU face threats from theft of intellectual property, targeted misinformation, attacks on critical infrastructure, and infiltration of social media platforms to influence democratic processes.

Digital sovereignty as ‘strategic autonomy’ favors exclusive control over European cyberspace. This involves EU developing a ‘hard power mentality’, as Arnout Molenaar, head of division in the European External Action Service, puts it (Csernatoni, 2021). This discourse draws on a long history of, particularly, French strategic thinking going back to the 1950s and further back (Gordon, 1993). Thus, Internal Market Commissioner, Thierry Breton, insists that a critical component of building trust in the data economy is creating rules to ensure that ‘highly sensitive data should be able to be stored and processed in the EU’ (Lomas, 2020). Arguably, certain data is only secure if it remains within European territory.

This raises a number of questions in relation to the prevailing idealization of the state as ‘a provider of individual security’ (Hansen and Nissennbaum, 2009, p. 1160). How should we understand the sovereign contract between state and individual if Gaia-X is the main security provider of the European sovereign cloud system? Will EU citizens hand over power (or rather data) to Gaia-X (and its partners) in exchange for the cloud’s protection of their security? Or rather, do sovereign ambitions of Gaia-X, like the spectre of an ‘EU army’ (Faludi, 2016), suggest that sovereign states pool
their sovereignty in Europe? In short, what happens to state sovereignty if the (data) security delivered by Gaia-X needs no state?

Cybersecurity

The competing conception of digital sovereignty in the security domain portrays sovereign control in terms of ‘cybersecurity’ (for debates on cybersecurity and the single market, see also Liebetrau, 2023). The idea, often promoted by transatlantic-oriented member states such as Sweden and Denmark, is that Europe can only be secure if intelligence information flows freely across the Atlantic. The cybersecurity approach to digital sovereignty sees territorialization as a threat to the integrity of data flows. From this perspective strategic autonomy undermines national sovereignty. Arguably, if Gaia-X becomes an autonomous, territorially exclusive cloud system, it risks preventing Europe from working efficiently with its most important allies (Mueller, 2020). Or, as MEP Axel Voss explains: if the choice is between being a colony of the US or a sealed European cloud, many will choose Microsoft (Voss, 2020). Unsurprisingly, this is tech giants’s favorite articulation of digital sovereignty. According to a Microsoft spokesperson, ‘in the cloud age […] it is wrong to define sovereignty solely along territorial borders’. Instead Microsoft and other tech giants could offer the ‘appropriate technological architecture’ to protect Europe’s coming cloud infrastructure from malicious actors.19

In the end, Gaia-X was opened for non-EU companies and secures the free flow of intelligence data among politically like-minded partners as long as EU law is respected. The point is to keep data within the reach of European and national jurisdictions, not territory.20

The strategic autonomy and cybersecurity conceptions of digital sovereignty approach territoriality differently. Either sovereignty only exists if data and infrastructure respect territorial integrity. Or territorial principles threaten digital sovereignty. In the latter interpretation, the lines of demarcation of Gaia-X should not follow territorial borders but jurisdictional borders, reflecting the transatlantic alliance structure and the technological superiority of US companies. While these articulations of Gaia-X may seem drastically different, their ontological assumptions are not. In both concepts, the state is not articulated as the security provider for its citizens. Instead, other referents, from post-national collectives to companies, do that job. As such, digital sovereignty challenges ideas of a national inside and an international outside.

**Digital sovereignty as economy**

In the economic domain, Gaia-X is seen to provide digital sovereignty either by enabling European tech champions to shield the EU’s single market from foreign companies or by boosting innovation by increasing competition with the rest of the world. In both cases, tech companies and markets rather than states are recognized as sovereign players in the data economy.

---

20 See: «https://www.gaia-x.eu/faq».
Neo-mercantilism

The first conception of digital sovereignty in the economic domain articulates the European data economy as independent from foreign companies. Europe should restrict access to its million-consumer market and rely on existing European providers or develop European alternatives. For example, according to Germany’s 2021 Data Strategy, Gaia-X is a means to ‘emancipate Europe from locked-in cloud services’ and achieve global dominance (Sahin and Barker, 2021). At the EU level as well, ‘Europeanizing the Gaia-X project’ is seen as one way to build an indigenous European cloud system instead of ‘replicating non-European hyperscalers’ (Voss, 2020, p. 13). Sovereignty in this respect is framed not just as market share but as a strategy to ‘reconquer’ spheres of influence, giving Gaia-X a neo-imperialist gloss.

Historically, John Agnew (1994) has argued, much thinking of national or global economy in terms of sovereignty is protectionist, and often implicitly mercantilist. Mercantilism was a set of practices and policies followed by many European states in the 17th and 18th centuries. Its most important characteristic was economic nationalism, based on the idea that the world’s wealth was fixed in size: one state’s gain came at the expense of another state’s loss. This policy was largely illusory, as economy and trade do not respect territorial borders. The EU’s single market, especially after the 1980s, is built on the idea that competition and liberalization will increase growth. However, as Agnew (1994) argues, in times of crisis and stagnation, protectionist ideas re-emerge. This is also the case when ‘digital sovereignty’ is understood in economic terms.
For French Minister of the Economy Bruno Le Maire, the 21st century’s economic value will be based on data, which is why it is essential to protect it. However, protection also means investing public money. Disappointed with the participation of the US and Chinese firms in Gaia-X, an Important Project of Common European Interest (IPCEI) — a special industrial policy vehicle - was launched in 2021, aiming at creating a European federated cloud exempt from state-aid restrictions. Yet, Gaia-X also receives public funds and protection from the liberal internal market. The use of public aid is defended by Europe’s accelerated adoption of cloud services for public administration, schooling, and healthcare. In this representation, the European economy is a society in need of protection, it is the constituted power, and the cloud becomes the solution, the constitutive power delivering digital sovereignty.

This protectionist sovereign cloud system is not a stable representation. For one, Gaia-X was initially framed as an attempt to avoid dividing Europe into 27 or more sovereign clouds — essentially a reaction to an upsurge of nationalism and protectionism. Moreover, Gaia-X ended up being open to foreign companies, including Amazon, Palantir but also Alibaba and Huawei. This openness to foreign companies led Yann Lechelle, CEO of French cloud provider Scaleway, to quit Gaia-X: ‘the pure intent of Gaia-X is unlikely to be achieved’. The pure Gaia-X protects and defends the sovereign European market, keeping foreign companies out.

22 All 27 member states have agreed to a 10 billion euro Alliance for Industrial Data and Cloud. See: «https://www.marketscreener.com/quote/stock/VMWARE-INC-58476/news/Sovereign-cloud-It-s-up-to-companies-to-lead-the-way-37031494/».
Market cosmopolitanism

This brings us to the second and radically different conception of digital sovereignty in the economic domain, aimed at increasing competition within the European cloud market. This version, which is gaining the upper hand, seeks to avoid an ‘EU protectionism light’ becoming a cover for state aid to an industry that is not truly competitive. Instead, it aims for what Parker and Rosamond call ‘market cosmopolitanism’ (Parker and Rosamond, 2013). In this representation, access is granted as long as EU rules and standards are accepted. By harmonizing regulations and liberalizing cross-border factor movements, European market integration is promoted, benefiting citizens as consumers. Following this understanding, the constituted sovereign is not the European data economy or a potential European tech champion, but anyone or any entity.

This conception resonates with the libertarian ideology that has long infused debates, including the Declaration of the Independence of Cyberspace, envisioning cyberspace as exempt from sovereignty (Barlow, 2019, p. 5-7). The economic sovereign could be a company, organization, or even a citizen. This version of market sovereignty is supported by EU medium-sized and smaller countries, fearing that Gaia-X will make bureaucracy more costly and restrict the free market logic further. As Carl Bildt, former Swedish Prime Minister, says, ‘you simply can’t regulate unicorns into existence’.24

24 See: «https://www.politico.eu/article/europe-ai-strategy-weakness/»
Instead, in the *market cosmopolitan* representation, both European start-ups and large foreign firms such as Microsoft, Google, and Amazon will be sovereign in their equal access to Gaia-X. This claim is reflected in Gaia-X’s official values, notably: ‘openness, transparency and interoperability’. The latter means that providers must ensure that customers can easily switch from one cloud provider to another without losing any data. The underlying idea is that interoperability leads to collaboration and scaling of business models, warding off the creation of monopolies. When promoting digital sovereignty, Gaia-X should therefore avoid introducing new market entry barriers. This way, Gaia-X attracts big companies, SMEs and start-ups, whether EU-based or not, and boosts innovation. Embodying the repository of sovereignty, these many sovereigns choose the policies they desire.

While neo-mercantilism and market cosmopolitanism promote different ideas of the data economy and Gaia-X, both conceptions avoid linking sovereignty to political authority. Instead, sovereignty is enacted when it ‘protects’ or ‘unlocks’ the value of national, corporate, and personal data. Digital sovereignty, is about innovation and competition. This stands in contrast to a conception of digital sovereignty, where rights are a constituent of sovereignty.

**Digital sovereignty as rights**

Much of the rationale underlying the idea of digital sovereignty in the EU is the need to preserve European values and rights. As European data are mostly processed and stored outside the EU, there are significant concerns about the loss of control over
sensitive and personally identifiable data. References to European norms and values are sprinkled all over descriptions of Gaia-X, and digital sovereignty is presented as a defender of the European way of life (Lambach and Oppermann, 2022). Of the three domains discussed in this article, digital sovereignty as *rights* is the most confusing and likely to be deluted. It is also the one that most explicitly questions territory as the basis of sovereign claims, illustrated by the dotted line in Table 1.

Two competing discursive claims can be derived from the dimension of rights drawing on different traditions of liberal political theory. They are either negative rights (i.e. the citizen’s right to be protected by fundamental European values of privacy) or positive rights (i.e. the right to share data not only with other European users but with the rest of the world). The first links digital sovereignty to personal rights as a citizen of the EU, the second advocates for sovereign data control across territories. In this case, we focus on Gaia-X’s ‘Self Sovereign Identity’ (SSI) as a lens into the tensions within and between these claims.

*Personal privacy*

The first conception expresses digital sovereignty as the individual’s sovereignty in the shape of rights over data and digital traces. The official presentation of Gaia-X alludes to this version with its emphasis on individual protection, a ‘human-centric version of cybersecurity’ (Diebert, 2018). It strives to ensure that all laws, policies,
and practices uphold the integrity of communication systems — from code to physical infrastructure and everything between, protecting data and users’ security, including encryption. As Angela Merkel explained: ‘I firmly believe that personal data does not belong to the state or to companies […]’ (Riley, 2020). Indeed, Gaia-X discourse emphasizes that all personal data has to comply with GDPR, linking the sovereign right to the notion of EU (extra)territorial jurisdictions, values, and subjects (Federal Ministry for Economic Affairs and Energy, 2020b). How is this done in practice?

In May 2022, Gaia-X released a proposal for how to promote ‘Self Sovereign Identity’ (SSI) — giving individuals control of their digital identities. Ideally, SSI provides individual control, security, and full portability (we will return to the latter). The individual (or organization) to whom the digital identity pertains, in other words, completely owns all data linked to it — no external party can claim to ‘provide’ the identity for them because it is intrinsically theirs. In this reading of digital sovereignty, the virtual self of the digital user becomes somewhat detached from a physical body, but not from the reach of European jurisdiction.

This stands in stark contrast to both the security and market versions of digital sovereignty, as the individual will be protected against both the state, market and companies (Pohle and Thiel, 2020, p. 59). However, creating this digital identity without relying on a third-party provider may be difficult to uphold (recall above, that 70 per cent of the cloud market is currently controlled by hyperscalers). Perhaps, then, the guarantees of the fundamental rights of individuals will be more oriented towards contributing to the EU’s internal market objective?
Data ownership

According to the second conception of digital sovereignty in the rights domain, users are not constituted as sovereign citizens because their data is protected, but sovereign in terms of whom they want to share data with. Here the idea is that individuals should have the right to benefit from their own data’s intrinsic value. The sovereign identity holder can also take a non-human form. Gaia-X’s white paper explains:

All participants in a Federation are empowered to exchange and validate credentials directly among themselves. With this approach, Gaia-X is a paradigm shift from today’s systems, where control of identity and information is either placed in the hands of a few or interoperability issues arise when multiple companies want to collaborate. With Gaia-X, people, organizations or machines [sic!] can self-sovereignly manage digital identities and associated credentials (Federal Ministry for Economic Affairs and Climate Action, 2022).

The vision is to correct the power imbalance between the data producer/holder by enabling the individual to gain possession of their data and determine their interactions with third parties on their own terms. Users will be able to lift and shift data among different Gaia-X providers.
Here digital sovereignty is not so much the EU citizen’s absolute right to privacy but more a universal capacity to sovereignly master digital data. In this version, digitally sovereign users can exercise their autonomy within the marketplace. This sovereignty is cast as apolitical, more akin to competence or digital literacy:

Gaia-X is open to all companies and organizations from all countries, […]. From start-ups to large enterprises, from universities to public institutions, everybody has the right and the responsibility to contribute (our italics) (Federal Ministry for Economic Affairs and Climate Action, 2022).

This raises several questions: Should one consider the digitally irresponsible citizen as essentially non-sovereign due to a lack of competence or political attitude? Is the citizen who does not want to share their data undemocratic and not interested in contributing to ‘public data commons’ (Zygmuntowski and Zoboli, 2021)? And what happens to broader societal concerns and political communities when sovereignty is so firmly claimed for individual entities, be they individuals, companies, or things? (Glasze et al, 2022, p. 22).

**Three scenarios: Constitutional tolerance, hegemony, or collapse**

Gaia-X reveals profound contradictions in the quest to make Europe digitally sovereign. Above we observed how the six competing conceptions of digital sovereignty are representative of a fractured and ambiguous political discourse, where sovereignty is promised to and from different actors and for various, often contradictory
purposes. What we are seeing is a moment of ‘sovereignty surplus’ in which competing interpretations create conflict (Walker, 2020). This contestation makes it possible to envisage different future scenarios. At this point in time, the conceptions are themselves so ambiguous that different actors with different agendas can promote the same one. Thus, the political work, including the lobbying of tech companies, involves appropriating and specifying these conceptions in ways that suit interests. Below, we sketch out three possible scenarios and their likelihood.

Constitutional tolerance

The first scenario is what we could call ‘constitutional tolerance’. Borrowing from legal theorists Neil McCormick and Joseph Weiler, constitutional tolerance is a meta-political principle expressed in the preamble to the EU treaty: ‘Determined to lay the foundations of an ever closer union among the peoples of Europe’. The determination to find a common way despite differences leads to an ‘equilibrium’. In this version, the six conceptions of digital sovereignty co-exist in representations of Gaia-X and the EU’s digital single market more broadly. Like previous controversial EU constructions that tinker with state sovereignty, such as the EU’s foreign service or the EU’s common border policy, Gaia-X and other digital sovereignty initiatives work exactly because of their ambiguity. Essentially, the ambiguity of the project may be its biggest strength.

Within the EU this is a familiar constitutional strategy. As Floridi has argued, this has ‘the advantage of feasibility and the shortcomings of a compromise’ (Floridi,
We may see various forms of ‘digital sovereignty-washing’ where the claim is articulated by companies and institutions, as a standard, but turns out to be empty in substance and impossible to implement. Others, on the other hand, have argued that constitutional tolerance is more demanding. It requires underlying commitments to common ideological constructs (Lawrence, 2019). Gaia-X has difficulties living up to such conditions. As Anthony Giddens writes, if Europe remains itself divided on digital politics, it may find itself once more ‘sandwiched between the US and China, with a digitally malicious Russia standing on the side-lines’ (Giddens, 2020, p. 6). In this scenario, the EU would have difficulties even holding on to its digital standard-setting power.

**Hegemony**

The second scenario is one of hegemony in which one particular conception of digital sovereignty gains a hegemonic position. While it may be tempting to imagine hegemony as more stable, this is not necessarily so. As Stuart Hall (1988, p. 7) puts it, discursive hegemony is ‘always contested, always trying to secure itself, always in process’.

If we were to imagine, for example, neo-mercantilism gaining a hegemonic position, it would not only have repercussions for the competing economic conception of market cosmopolitanism, but also for digital sovereignty conception in the security and rights domain. Sharing data with intelligence services outside of the EU, including
the NSA, would become more complex, and giving data rights to non-EU companies and individuals would equally be problematic.

Similarly, if the individual privacy concepts prevails, it will have repercussions not just in the rights domain, but for both security and market domains. As some argue, the only way the cloud can deliver full sovereignty is if data is operated by trusted institutions in multiple countries and industries, forming a decentralized network much like the Internet itself. Here the tensions are evident. In this scenario, the EU would appear more united to the rest of the world, but it would require much internal political debate.

**Collapse**

The third scenario is *collapse*: The weight of irreconcilable versions of digital sovereignty may make the agenda crumble (Lambach and Opperman, 2022). Such a collapse need not be dramatic. Governments may be ‘put off’ by suggestions of European digital sovereignty and gradually work to erode it from the inside. For example, a claim to digital sovereignty in the security domain — both as strategic autonomy and cybersecurity — may over time undermine the understanding that digital sovereignty is a right to integrity and self-ownership. Interestingly, this scenario will not necessarily diminish the EU’s geoeconomic power. Instead, a collapse may enable the EU to pursue more targeted interests, partly freed from the constraints of having to deliver something as difficult as sovereignty. In that case, however, they
may need to defend the disappearance of 'digital sovereignty' form official discourse, which, we argue below, may cause even greater problems.

* A superficial geopoliticization?

Which scenario is most likely? Similar to Herranz-Surrallés, Damro and Eckert (2024), we see a split in the digital sovereignty debate between an ‘open’, post-territorial digital sovereignty agenda, akin to the idea of ‘open strategic autonomy’, and a more territorial, protectionist, and Europe-focused agenda. We currently find that Gaia-X is more inclined towards the open version, adding tech policy as another domain affected by ‘superficial geopoliticization’ (that is, change in discursive representations more than in practical policy and processes). In the context of the digital single market, the EU thus also faces a ‘geoeconomic dilemma’ (Herranz-Surrallés, Damro and Eckert 2024) between protection and advocating for an open global economy.

The break with the EU’s previous digital agenda, emphasizing free trade and global competition, may thus be overstated (Celeste, 2021, p. 216). The direct involvement of foreign tech players in the construction of industrial data spaces suggests that the digital sovereignty agenda is as much about control as it is an adjusted version of market cosmopolitanism (Baur, 2023).

Yet, even ‘superficial geopoliticization’ will have tangible effects. One likely outcome is a ‘Brussels effect 2.0’. Indeed, Gaia-X is already compelling US cloud providers to
spell out how they will protect customer data in Europe.26 The European Commission (with initiatives like the EU Cloud Rulebook) and single member states seem focused on this agenda, indicating that the EU will continue to project its regulatory effect abroad through e.g. cloud standards. However, our analysis also suggests that other concepts of digital sovereignty — those related to security and rights — could come back to haunt the EU. Ultimately, their political salience will obscure internal debates and frustrate the promotion of an open digital market, regulated by EU standards.

Conclusion

In the EU, digital sovereignty is more than a call for taking back control of data. It is part of a broader geopolitical agenda, positioning the EU in an economic rivalry between the US and China, and infusing debates about the future of the (digital) single market with connotations of power, authority and democratic values.

We approached digital sovereignty as a contested and contestable claim in a discursive and performative sense. It is precisely because of its ambiguity and malleability that digital sovereignty can rally many different actors and competing positions (Lambach and Oppermann, 2022). We showed this complexity in the analysis of a single case, Gaia-X, where we identified six distinct claims to digital sovereignty articulated across the domains of security, economy, and rights. The debate is further split between territorial (strategic autonomy, neo-mercantilism, and personal privacy)

and post-territorial (cybersecurity, market cosmopolitanism, and data ownership) concepts of sovereignty. The latter, which appears to be the most dominant, insinuates a significant reconfiguration of sovereignty in the EU. In all three post-territorial concepts, the sovereign line does not necessarily coincide with the line separating one polity from another. Across the six different concepts, the cloud infrastructure and companies perform as state-like providers of security, growth, and, indeed, sovereignty (Fairbank, 2019; Smith, 2017). Meanwhile, the power and authority that digital sovereignty claims articulate are capable of being enacted by a variety of human and non-human agents. As a result, it is uncertain how, for instance, data sovereignty for individuals or virtual selves can be reconciled with cross-border data flows and digital trade within Gaia-X, the single market, or globally.

We developed three scenarios to consider what this discursive struggle may mean for the EU’s future. In both the constitutional tolerance and collapse scenarios, digital sovereignty may end up emptying itself of political potency. Even in a scenario of hegemony, where one version gains dominance in the EU, sovereignty takes on qualities of management with expertise and technical skills, rather than clear political visions for the EU. The initial geopoliticising pressures to shield the EU’s cloud market from foreign dominance have been replaced by the pragmatism allowing foreign tech giants to partake in the development of Gaia-X. Here, the many digital sovereignty concepts obscure rather than clarify the EU’s power, control, and authority.

Once sovereignty has been promised, it is difficult to take back. The concept exerts its own ‘gravitational pull’ (Lambach and Opperman, 2022, p. 13). This leads us to
conclude that the EU is unlikely to go back to its earlier eliminate-all-barriers-to-trade approach in the digital single market.

Our discursive analysis of Gaia-X reiterates the fact that words matter in politics, as they create expectations and perform possible worlds into existence. Digital sovereignty of any shape or form eventually leads to expectations from states, individuals, civil society, and companies that they — or someone else — reclaim ownership. This *geopoliticizes* the digital single market. As such, even if the current project crumbles, digital sovereignty has already shaped the EU and its role in the (digital) world. It is unlikely that a unifying understanding of digital sovereignty will be found any time soon. Important political work will take place in its specification and implementation. It is therefore high time that we think more about which concept of digital sovereignty we want to promote.

**References**


Lomas, N. (2020) ‘Europe’s data strategy aims to tip the scales away from big tech’, 24 November. Tech Crunch: «https://techcrunch.com/2020/11/24/europes-data-strategy-aims-to-tip-the-scales-away-from-big-tech/?guce-counter=1&guce_referrer=aHR0cDovL2luZm8uaWFwcC5vcmcv&guce_referrer_sig=AQAAAGJAbfc2Jph0Yk8y2iAPf48nVAhnY7gf894rBlEUM_nDsrktt-mFRqwYX8mo697JLbDUdaDCL-_BQKa0M-QVZbt0b4tUCjL8iAL8VmuDrHN94_IuazjvzyAq0gJhh5RWW-fIIcPrI9KL2r0333vcgX7xfEVrTpdPdw0RL8K0KOwg».


