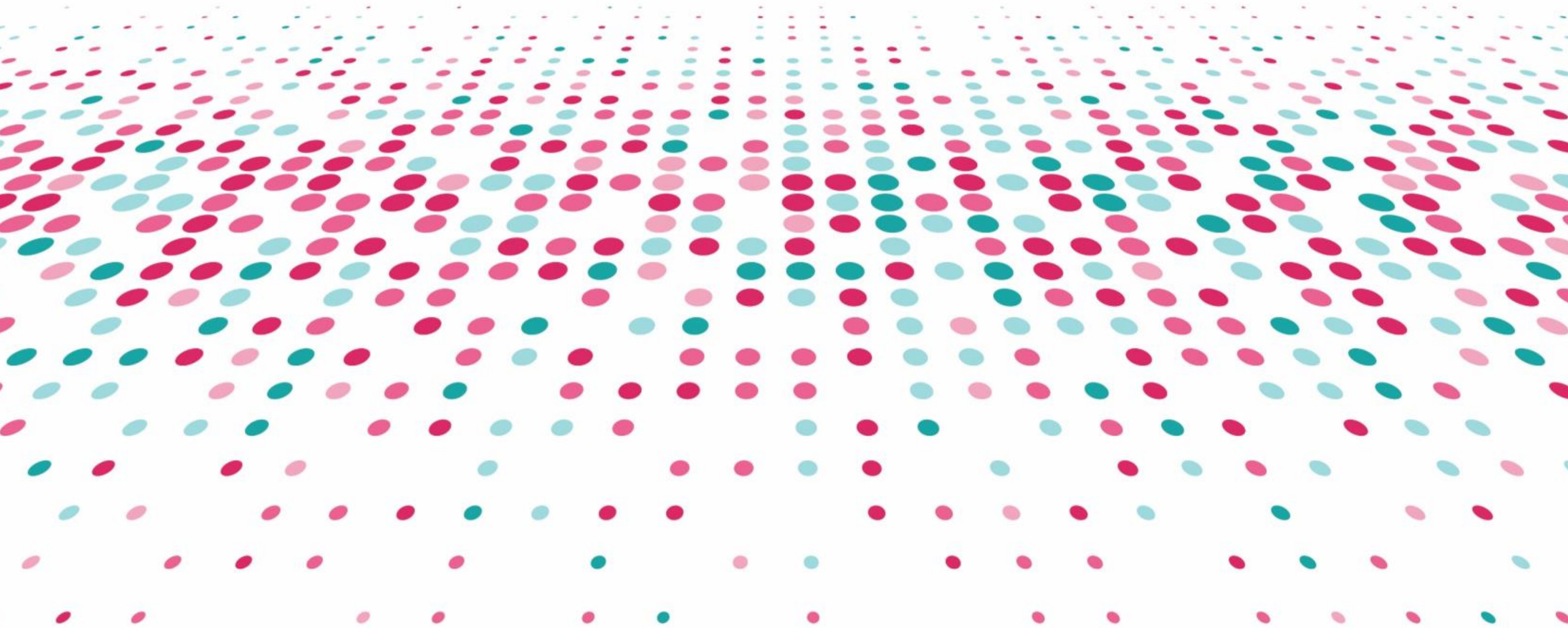
European Commission

European DATA Market Study 2021–2023

CNECT/LUX/2020/OP/0027–VIGIE 2020-0655, contract number: LC-01568518



Story 4 – Digital Sovereignty in the EU: A convoluted Journey

Update of the European Data Market Study 2021-2023
VIGIE 2020-0655

May, 2023

IDC

the Lisbon council
think tank for the 21st century

Author(s)	Giorgio Micheletti, Nevena Raczko (IDC)
Deliverable	D3.4 Quarterly Stories (Story 4)
Date of delivery	
Version	0.3
Addressee officer	Katalin IMREI Policy Officer European Commission, DG CONNECT Unit G1 — Data Policy and Innovation EUFO 1/178, L-2557 Luxembourg/Gasperich katalin.imrei@ec.europa.eu
Contract ref.	LC-01568518

CONTENTS

List of tables

EXECUTIVE SUMMARY

This paper proposes an overview of the concept of digital sovereignty and attempts an analysis of its practical dimensions in Europe today leveraging both the emerging academic literature on the topic, as well as the results of in-depth interviews with key stakeholders involved in the design and implementation of digital policies. Through extensive desk research and literature review, complemented by in-depth interviews with representatives of industry associations, academia and think-tanks and private organisations, the aim of the research is to apprehend the concept of digital sovereignty, as well as its consequences and impacts on the data economy, along the different perspectives of a varied set of stakeholders.

The notion of digital sovereignty is not new as the term has started to arise in the academic and political debate in ethe early 2000s. The concept has gained in popularity with the introduction of the Digital Agenda for Europe, and it recently re-surfaced as a means of promoting European leadership and strategic autonomy in the digital field. As such, digital sovereignty now features prominently in the Von der Leyen’s Commission political priorities and is sparking hefty debates among policy-makers, scholars and businesses. Yet, the concept is still ambiguous and not univocally understood: it may refer to the creation of research and development (R&D) competencies by maintaining a strong knowledge base in critical digital technologies; it may represent the achievement and preservation of a leadership position in key digital technologies to turn R&D into market products; or it can revolve around the development of adequate policies and standards that ensure digital autonomy while influencing global regulations, standards and practices.

Our stakeholders’ analysis also revealed a multitude of views on digital sovereignty. Trade associations and industry representatives, for example, tend to highlight the need for Europe to maintain innovation potential without cutting fundamental cooperation exchanges with other players on the global stage. Research and academia, on the other hand, insist on the need to achieve political and economic autonomy in the EU and at Member State level vis-à-vis Europe’s partners or competitors. The private sector welcomes a regulatory stance by national and EU institutions provided that this interventionist approach does not undermine Europe’s capacity to remain open, competitive and able to innovate. Member States too appear to have different positions vis-à-vis digital sovereignty initiatives. Countries like France and Germany have demonstrated to appreciate the design and implementation of prescriptive policies and have fruitfully initiated a close collaboration around different themes with the GAIA-X project on the forefront. Other Member States (often smaller Member States with more open economies) see potential risks linked to a top-down approach to digital sovereignty imposed at the EU level. Deprived as they are of a strong technology industry, their access to cutting-edge digital developments, new economic opportunities and productive partnerships with non-EU members could in fact become more problematic.

In view of these definitional ambiguities, the present research suggests the adoption of an empirical definition articulated along a three-dimensional framework:

- the **privacy and data protection dimension** of digital sovereignty axed on the ability for European organisations and citizens to control their own data and digital lives;
- the **cybersecurity dimension** of digital sovereignty centered on the need to promote a unified and effective cyberspace to counter Europe’s digital structure overdependence on few and non-European technology providers;
- the **strategic/geopolitical dimension** of digital sovereignty with the aim to promote a European alternative to the EU’s economic and ideological rivals in the digital space at global level.

In this context, the view of the business sector comes also into play. For instance, the growing extraterritorial application of data governance laws is subjecting organisations to an increasing tension between enabling digital innovation associated with cloud and ensuring that data and IT infrastructures are compliant with regulations and guidelines. As a result of these tensions - and given the complexity of making risk assessments on third-country laws and practices and the need for additional technical safeguards - data localization is often the only practical option for businesses. It is not surprising therefore that 64% of organisations polled for an IDC survey cited adopting a risk mitigation approach to either holding or migrating GDPR-governed data to datacenters in Europe while around 42% of European organisations opted to undertake greater due diligence of their cloud service providers to determine local hosting capabilities and the adequacy of their legal, privacy, and security safeguards. All in all, however, our research reveals that the vast majority of businesses in Europe (69%) agree that digital sovereignty initiatives, enchance customer, partner and government trust in their organisations and ultimately contrinute to strengthen their company's resiliency.

As a final remark, and despite these apparent challenges, the European Commission is successfully pursing its efforts towards a more digitally sovereign Europe along the lines of the EU Digital Strategy and the European Strategy for Data.

▶ INTRODUCTION

Background

The EU plays a pivotal role in creating the necessary framework conditions for effective technology generation, development and diffusion in Europe. At the same time, the way digital technologies are applied and regulated across the EU exerts a strategic influence on the empowerment of the Union as a whole, both externally and internally. Externally, the EU could continue to serve as a model on the international scene in governing digital transformation (Bradford, 2020; Rhinard, Stoestedt, 2019). Internally, the disruptive innovation potential brought about by digitalisation could not only affect Europe's social and economic welfare (Anderton, 2020), but also influence the long-term process of European integration, hence impacting the dynamics among the Member States and between the Member States and the EU as a whole (Massaro, 2019).

While the EU has long been ahead of the game compared to the U.S. and other key international players when it comes to regulating the digital world, (for example in data protection, privacy and human rights law[1] or in ensuring a higher degree of digital market competition[2]), the actual implications of this proactive stance have not always been easy to assess (Brauer and Erixon, 2016). However, the current implementation of the **EU Digital Strategy**[3], and the concrete policy steps undertaken by the new **European Data Strategy** in the period 2020-2022[4], are raising promising expectations on Europe's ability to become a truly global digital leader – in other words, to become *digitally sovereign.*

Indeed, the EU and its Member States are facing an increasingly complex context of international relations and geo-political tensions. This was acknowledged from the beginning by the von der Leyen Commission. President von der Leyen made it clear during her first press conference that she would be in charge of a "geopolitical Commission."

This context must be considered when interpreting contemporary positions on "digital sovereignty" and "strategic autonomy" in the EU. The COVID-19 emergency has not only sped up the digitalisation process and shown how important our ICT infrastructure is, but it has also raised awareness of the negative effects of relying on foreign suppliers for essential services and goods. Thus, the pandemic also accelerated the trend towards gaining strategic autonomy with policymakers in the major economic blocs globally (US, Asia and Europe). Given the prominence of digitalisation during the pandemic, it is not surprising that within the public debate around strategic autonomy, "*digital sovereignty*" is often in the spotlight. As part of the wider debate, **digital sovereignty tends to refer to concerns about the autonomy of crucial national ICT infrastructure and the control individuals have over their own data**. These concerns emerge from an ever-growing importance of digitalised critical infrastructure, an increasing centrality of mobile telecommunications networks for the functioning of businesses and

[1] See for instance the EU General Data Protection Regulation (GDPR), https://gdpr.eu/

[2] See the Digital Markets Act (DMA), https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

[3] European Commission "Shaping Europe's Digital Future", COM(2020) 67 final, 29 February 2020 https://digital-strategy.ec.europa.eu/en

[4] In the period 2020-2022, the European Commission has proposed different measures under the European Strategy for Data (A European strategy for data (COM(2020) 66 final, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en) on how to regulate Big Techs, ensure cross-sectoral data flows, and increase usage and re-usage of data between businesses, governments and citizens.

society as well as an apparent lack of control over data on both the individual and the collective (national and supranational) levels. Despite the underlying incompatibility between digitalisation and sovereignty in the conventional sense (i.e., digitisation being an inherently borderless phenomenon while sovereignty being directly linked to a territory), Europe's policy-makers are becoming more vocal on regaining control over a transition that is led by companies with non-European roots.

The state of the art of the public debate on digital sovereignty is therefore extremely varied. Several dimensions of the concept have been put forward over the past few years and other interlinked conceptualisations (such as *technological sovereignty* or *strategic autonomy*, to name a few) have emerged and can be considered closely interwoven with the notion of sovereignty in the digital space. These concepts are often used interchangeably. The view adopted by this paper is that they refer to different, interlinked dimensions of the very notion of digital sovereignty purported by this research, i.e. a three-dimensional framework where digital sovereignty encompasses a) the privacy and data protection dimension; b) the cybersecurity dimension and; c) the strategic/geopolitical dimension. European technological sovereignty, for example, is often presented as *Europe's ability to develop, provide, protect and retain the critical technologies required for the welfare of European citizens and prosperity of European businesses, and the ability to act and decide independently in a globalised environment* (Ramahandry *et al*, 2021). In this respect, elements of technological sovereignty are visible in all the three dimensions of digital sovereignty with particular reference to the cybersecurity and, to a lesser extent, the privacy and data protection dimension. Strategic autonomy, on the other hand, falls more clearly under the geo-political dimension as it refers to the *capacity of the EU to act autonomously – that is, without being dependent on other countries – in strategically important policy areas*. *These can range from defence policy to the economy, and the capacity to uphold democratic values*[5].

This paper proposes an **overview of the concept of digital sovereignty and attempts an analysis of its practical dimensions in Europe** today leveraging both the emerging academic literature on the topic, as well as the results of in-depth interviews with key stakeholders in the past few months.

Methodology

For the realization of this story, the study team has conducted desk research on a set of IDC sources and publicly available documents (see the list in the Bibliography section). The desk research was accompanied by an additional effort of primary research in the form of in-depth interviews with companies and organisations that are active members of the European digital stakeholder ecosystem. In-depth interviews were conducted between March and May 2022 with representatives of industry associations, academia and think-tanks with the aim to apprehend the concept of digital sovereignty, as well as its consequences and impacts on the data economy, along the different perspectives of the different stakeholders.

The interviews set out to address the following questions amongst others:

I. The concept of digital sovereignty: which components (business, industry, citizens, society, technology, infrastructure, ethical/trust, etc..) are part of it and how is the EU dealing with these components;

II. Focus on economic, business and industry implications of digital sovereignty in practice for the EU: what do you see from your privileged observation point and is the EU doing too little or, conversely, is the EU pushing digital sovereignty too far.

III. Adequacy of means: the EU is fostering digital sovereignty, but does it have the necessary resources (in terms of technology generation and uptake capacity, available infrastructure, cybersecurity and safety, measures in place, available skills) in place to actually achieve a true and complete digital sovereignty?

[5] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733589/EPRS_BRI(2022)733589_EN.pdf

IV. Desirability of results: is in the end digital sovereignty a good thing for the EU? Could the EU approach be turned into a protectionist exercise with negative consequences for the EU economy as a whole and for some Member States in particular (e.g. those with a more liberal/open economic tradition)? Is real digital sovereignty a rear-guard battle? Is itoo late for the EU to catch up and wouldn't it be better to increase cooperation with the US (and/or China)?

This research process resulted in the identification of key stakeholders, each bringing a unique perspective and offering a cross-sectoral view to this story.

- **Trade Associations**:

Bitkom[6] is a German digital association. Bitkom promotes the digitalization of the government, society, and the economy. Bitkom promotes policies for platforms, disruptive technologies, work 4.0, lifelong learning in a digital age, data-driven business models, data protection, and cybersecurity. The core of Bitkom's interests are a strong European digital policy and a fully integrated digital single market, as well as positioning Germany as a major force for global and European digital development.

- **Academia:**

The *United Nations University – Maastricht Economic and Social Research Institute on Innovation and Technology (UNU-MERIT*[7]*)* is a research and training institute of the United Nations University (UNU) which collaborates closely with Maastricht University. UNU-MERIT aims to advance societal policy and innovation research, provide education and mobilise knowledge in order to unlock the full potential of innovation for achieving inclusive sustainable development. The research agenda of UNU-MERIT on 'Comprehensive Innovation for Sustainable Development' (CI4SD) focuses on the interconnected risks and opportunities of innovation, as they relate to climate change, digital transformation, poverty and inequality, migration and population, and the future of work.

- **Research Institutes**:

The *Fraunhofer Institute for Software and Systems Engineering ISST*[8] identifies and realizes the strategic value of data in cooperation with companies. The Fraunhofer ISST teams research the value and sovereign handling of data for logistics, healthcare, and the data business. We develop solutions for data management and the establishment of data architectures.

- **Think Tanks**:

CEPS[9] is a leading think tank and forum for debate on EU affairs, ranking among the top think tanks in Europe. At CEPS, researchers perform policy research on a wide range of policy areas: from the economy and finance to better regulation, the digital economy and trade, as well as energy and climate, education and innovation, foreign policy and the European integration process, or justice and home affairs.

[6] https://www.bitkom.org/EN/About-us/About-us.html
[7] UNU-MERIT
[8] Fraunhofer Institute (fraunhofer.de)
[9] About CEPS – CEPS

- **Private sector**:

Microsoft's[10] work in Brussels is focused on creating the right frameworks to ensure that every European can make the most of digital opportunities, without compromising on the fundamental values which underpin our societies. Microsoft participates in discussions about a variety of policy topics, such as data security, sustainability, accessibility, and digital skills. The interviews were followed by a set of concluding remarks where the key messages from the interviews and case studies were summarised, contrasted and compared and some essential policy considerations outlined.

The main data sources used for the realisation of this research are summarised in the table below and in the bibliography at the end of this document.

Table 1 Data Sources

Data Sources	Description
Secondary data sources	• Academic publications and policy reports (see bibliography and footnotes)
Semi- structured interviews (Duration average 45-70min)	• Policy Office, EU Data Economy • Information Specialist and Researcher at UNU-MERIT • Researcher • Full Professor • Senior Director, EU Government Affairs

DIGITAL SOVEREIGNTY: AN OVERVIEW

Digital Sovereignty – A concept coming from afar and its relevance today

The need for countries and supra-national institutions to act independently and autonomously in the digital world can be traced back to the mid-1960s (Kuo, 2022). Still, the actual term digital sovereignty arose only in the early 2000s (Drouillat, 2014) and was tentatively defined for the first time in 2011 (Bellanger, 2012). The concept gained in popularity with the introduction of the Digital Agenda for Europe (European Commission, 2010b) and it recently re-surfaced as a means of promoting European leadership and strategic autonomy in the digital field (Lippert et al., 2019). As such, digital sovereignty now features prominently in the Von der Leyen's Commission political priorities and is sparking hefty debates among EU institutions (EPCS, 2019), scholars (Floridi, 2019), citizens, businesses, and Member States (Madiega, 2020).

Starting with concerns expressed first by France and, later, by Germany, the EU's engagement with the concept of digital sovereignty has been the result of the Member States upgrading their understandings of the role of the digital world in the context of the international system (Bellanova *et al*., 2022). At Member States level, the gradual awareness within French society that citizens' personal data were being accessed, transferred to, and processed by US-affiliated companies gave rise to feelings of loss of control over that data and promoted an important mediatic debate. What is more, this perceived loss

[10] https://blogs.microsoft.com/eupolicy/microsoft-in-brussels/

of control was linked to economic anxieties over market dominance by large foreign corporations such as Google, Amazon, Facebook, Apple and Microsoft (also popularised as GAFAM), which were understood as reducing the industrial and economic development of France, transferring added value abroad and limiting the capacity for innovation (Floridi, 2020). As a response, the French government adopted a more interventionist and localized approach aimed at regulating the exchange of copyrighted material online or address cyber-crime (the Hadopi Law of 2009 and the LPPSI 2 Law of 2011). Attempts to create local solutions also included projects aimed at competing with US cloud computing technology, such as Andromède (2009), Cloudwatt (2012) and Numergy (2012) (Gheham, 2017). In Germany, the debate revolved around similar concerns, although the country focused also on the importance of protecting national IT infrastructure from external interference, developing counter-surveillance technologies, reducing the transfer of data beyond EU borders and decreasing technological dependency on non-EU countries by encouraging the creation of national IT products (Pohle, 2020).

Perhaps the most interesting consideration about the Franco-German engagement about digital sovereignty is that this Member State dynamic strongly helped shifting the debate to the EU playing field, recognizing that the best way to achieve real sovereignty in the digital domain was by working together at European level (see on this point the declaration of the French Minister of Culture, Catherine Morin-Desailly in 2013 and of Thomas de Maizière – Germany's Minister of the Interior – on the same year)(Steiger et al., 2017). As a result, throughout the Juncker Commission (2014–2019), it was already possible to observe a nascent EU discussion that, not only reflected the concerns expressed by France and Germany (economic, data protection, EU values and security), but also reacted to a number of external events and processes such as the Snowden revelations and foreign interference with democratic elections and referenda (Pohle and Thiel, 2020).

The arrival of the von der Leyen Commission marked a gear-change towards a more structured and strategic thinking about digital sovereignty, thus positioning the concept at the heart of the EU integration project (Bellanova *et al*., 2022). Ursula von der Leyen asserted from the start that "Europe must lead the transition to a [...] new digital world, by gaining technological and digital sovereignty" in her vision for the 2019–2024 Commission. Indeed, the political guidelines that she set related closely to the topic of digital sovereignty as she pointed out that "[...] it is not too late to achieve technological sovereignty" referring to areas including blockchain, high-performance computing, quantum computing, algorithms and tools allowing data sharing and data (re-)use[11]. Similarly, the Commissioner for the Internal Market, Thierry Breton, argued for a Eurocentric technology agenda insisting that "[...] this is not a protectionist concept, it is simply about having European technological alternatives in vital areas where we are currently dependent." The Data Act proposed in February 2022 and the Data Governance Act that entered into force in June 2022[12] reflect this understanding. Both legislative initiatives, have been developed with the fundamental objective of promoting the availability of data and creating a reliable environment that facilitates its use for research and the creation of new innovative services and products and they are relevant components of a bigger legislative plan, the European Data Strategy13 which aims to strengthen the data economy. On the one hand, the Draft Data Act aims to maximise the value of data in the economy by ensuring that a wider range of stakeholders gain control over their data, and that more data is available for innovative use, while preserving incentives to invest in data generation. On the other hand, the Data Governance Act refers to a set of rules and means to use data in a secure way, including through trusted third parties. The Digital Governance Act seeks to add an addtional layer to data transfer regulation with respect to non-personal data with the aim of safeguarding public-sector data, data intermediation services, and data altruism organisations against unlawful international transfer of, or governmental access to, non-personal data. In particular, Article 31(1) of the act requires public sector bodies, data intermediation services, and recognised data altruism organisations to take all reasonable technical, legal, and organisational measures, including contractual

[11] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf, page 13.
[12] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
[13] https://digital-strategy.ec.europa.eu/en/policies/strategy-data

arrangements, in order to prevent international transfer or governmental access to non-personal data held in the EU where such transfer or access would create a conflict with EU law or Member State Law. The same article envisages a coercive measure in the hands of Member States to make sure that such non-personal data transfer or access is avoided. The article further states that fines are to be set and implemented by each Member State so that they are 'effective, proportionate and dissuasive'. Unlike the GDPR, the DGA does not prescribe the specific amounts and weighting factors applicable to the corresponding monetary sanctions.

The proactive attitude of the von der Leyen Commission comes at a time when US corporations dominate the EU's cloud industry and have unparalleled access to the personal information of EU individuals thanks to online platforms fed by online advertising (such as social media). Accordingly, one of the first EC-led policy initiatives echoing this push towards the provision of digital tools originating in the EU was the plan to create a series of common European data spaces[14] with the aim to achieve in due course a single European space where data can be shared and used freely and safely by a multitude of stakeholders. Eventually this will trigger the creation of an EU designed single market for data that shall enable EU companies (and in particular SMEs) to reap the benefits from data which would otherwise be difficult or impossible for them to access. The European Strategy for Data[15] outlined the concept in detail while Thierry Breton summarised its goal as follows "[...] European data will be used for European companies in priority, for us to create value in Europe."[16] Digital sovereignty, in other words, is the strategy that will allow the EU to drive economic and industrial development, to protect EU citizens' data, to guarantee EU fundamental rights, and to secure physical and information-critical infrastructures – ultimately, we could add, digital sovereignty could represent another step forward on the long and bumpy road to European integration.

Digital Sovereignty – a multifaceted concept

While certainly captivating, the notion of digital sovereignty is still ambiguous and not univocally understood (Pohle and Thiel, 2020; Crespi *et al*., 2021): it may refer to the creation of research and development (R&D) competencies by maintaining a strong knowledge base in critical digital technologies; it may represent the achievement and preservation of a leadership position in key digital technologies to turn R&D into market products; or it can revolve around the development of adequate policies and standards that ensure digital autonomy while influencing global regulations, standards and practices (Timmers, 2022). The policy initiatives put in place by the European Commission over the past couple of years have spanned all these elements of digital sovereignty with the aim to establish Brussels as a global first mover on tech regulation. This in the hope to endow the EU with a new international assertiveness and curb foreign companies' dominance over vast sections of Europe's digital space (Kalff; Renda, 2019).

To navigate the ambiguity surrounding the notion of digital sovereignty, the present research suggests the adoption of an empirical definition put forward by a recent study benchmarking digital sovereignty initiatives across the EU Member States[17] since 2018.Baischew *et al* propose a three-dimensional framework to tackle the topic: **a) the *privacy and data protection* dimension**, **b) the c*ybersecurity* dimension** and **c) the *strategic/geopolitical* dimension**. Whilst the first dimension revolves primarily around the individual ability to control one own's data and digital lives, the second and third dimensions refer mostly to the power by Member States and the EU to (re-)gain control in the digital age. The

[14] https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces
[15] European Commission (2020): A European strategy for data. COM(2020) 66 final.
[16] EC AV PORTAL (europa.eu)
[17] Baischew, D.; Kroon, P.; Lucidi, S.; Maerkel, Ch.; Soerries, B. (2020). Digital Sovereignty in Europe – A first Benchmark, WIK Consult, Report, December 2020

privacy dimension of digital sovereignty entered the European policy debate with the increasing adoption and dominance of US consumer-oriented online services offered at no monetary cost in the EU through the use of personal data of millions of European citizens. The second dimension around cybersecurity emerged with the realization by European policy-makers that fundamental elements of the Europe's digital infrastructure (5G, cloud computing, edge computing, for example) present critical weaknesses because of the absence of a unified cyberspace and due to the over-dependence on few (non-European) equipment suppliers. The third dimension on the strategic importance of digital sovereignty for the EU has been emphasized by the general "geopolitical" stance of the von der Leyen Commission, which has advanced the debate with the aim of sustaining a European alternative to its main economic and ideological rivals on the global stage. In this paper, we follow this three-dimensional approach to identify the advances and obstacles on the path to digital sovereignty in Europe until today.

EU DIGITAL SOVEREIGNTY IN PRACTICE: UNEVEN PROGRESS AND OBSTACLES AHEAD

The Privacy and Data Dimension of Digital Sovereignty

The economic model employed by some of the key "Big Techs" is largely based on the collection and exploitation of online users' data in order to generate advertising revenue. Technology companies are therefore collecting enormous amounts of personal data. The Cambridge Analytica incident showed how online platforms may also collect personal information for the aim of political profiling. In the end, these tendencies—often referred to as surveillance capitalism[18] (Zuboff, 2019)—lead to European individuals progressively losing control over their private information. Concern has grown in the EU as to how European citizens can recover control of their digital data (or 'trace') in an online environment that is now largely dominated by non-EU tech companies. A recent example is the controversy concerning the development of contact-tracing solutions for controlling the spread of coronavirus. The technological choices made by Apple and Google have frustrated the ability of some Member States to design their own contact-tracing solutions (such as 'Stop Covid' in France) and fuelled the quest for digital sovereignty[19]. In a post-coronavirus pandemic world, where technology will no doubt play a more crucial role, the challenge remains for EU policy-makers to find the right balance between control and privacy rights while, as stated by Commission Vice-President Margrethe Vestager, EU citizens want to trust technology when they use it and not begin a new era of surveillance.

With the General Data Protection Regulation (GDPR) at its core, the EU has implemented an exceptionally strict framework for privacy and data protection. To increase peoples' control over their own data, the EU also introduced a protective "right to be forgotten" and a data portability right. Furthermore, the Commission has set out a strategy on promoting international data protection standards. A specific case in point, have been the disputes on an adequacy the decision regarding the transfer of personal data from the EU to the US. The adequacy decision on the EU-US Privacy Shield was adopted in 2016 and allowed the free transfer of data to companies certified in the US under the Privacy Shield. In 2020, the Court of Justice of the European Union invalidated the adequacy decision thus making the EU-US Privacy Shield null and void. The process was resumed in December 2022 when the European Commission published a new draft adequacy decision on the future of international data transfers with the United States. One of the key elements underlying the Commission's draft adequacy decision is the fact that American companies will have to commit to comply with an exhaustive set of privacy obligations, if wanting to partake in the EU-US Data Privacy Framework. More concretely,

[18] Harvard professor says surveillance capitalism is undermining democracy – Harvard Gazette
[19] See La Tribune, Terminal neutrality as a tool for our digital sovereignty?, 2020.

these privacy obligations entail that US companies will be required to "delete personal data, when it is no longer necessary for the purpose for which it was collected, and to ensure continuity of protection when personal data is shared with third parties."[20] In its Opinion of 28th February this year, the European Data Protection Board welcomed the improvements included in the new draft adequacy decision but also pointed to concerns and requested clarifications in particular on certain rights of data subjects, onward transfers, the scope of exemptions, temporary bulk collection of data and the practical functioning of the redress mechanism.

Data access from third countries' governments has also been part of the European Commission's legislative measures. The already mentioned Art. 31 of the Digital Governance Act for example prevents international transfer or governmental access to non-personal data held in the EU and Art. 27 of the proposed Data Act puts in place safeguards to address unlawful third-party access to nonpersonal data held in the EU. The proposal requires data processing service providers to implement a set of technical, legal and organisational measures to handle access requests from authorities in non-EU countries to non-personal data held in the EU.

Thanks to this proactive stance, the EU is seen as a standard-setter in privacy and data protection at global level, with various countries having incorporated GDPR provisions into their national legislation and some multinationals having opted to adopt GDPR as their global standard of operation. While EU Member States are considering adopting location-tracking methods to stop the virus's spread, the coronavirus outbreak presents a true test for the EU framework. The EU institutions have been instrumental in fostering the development and use of technical solutions that abide by the stringent EU privacy standard, such as the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) system (Obendiek, 2022). The EU has also used a soft law approach to ask telecom firms to hand over anonymised mobile metadata (to help analyse patterns of coronavirus contagion) and adopt guidelines and a toolbox for developing coronavirus-related apps that provide sufficient data protection and limit intrusiveness. The EU will further scrutinise contact-tracing technology proposed by Google and Apple, to ensure it meets the bloc's new standards.

The actions outlined above demonstrate, if still necessary, the EU potential as a leader in data collection and data processing on a global stage. Creating a solid EU data framework is precisely the way that the Commission has undertaken to assert its leadership in this field. This will make it easier for innovators to secure access to data, notably in the business-to-business (B2B) or government-to-citizens (G2C) sectors. Building an EU data space would depend on granting open access to government data in certain strategic industries, such as transportation or healthcare, enabling businesses to access marketplaces for data while protecting their privacy, and promoting data sharing. These actions are in fact all in line with the European data strategy. Furthermore, reflecting on solutions to fostering public data collection at intra-national level would be useful. An interesting example is provided by the experiment conducted by the city hall of Barcelona, which included a 'data sovereignty' clause[21] in public procurement contracts requesting its partners give back the data they gather to deliver services to the city in machine-readable format. Should such clauses prove useful, best practices could be further identified and applied at EU level.

The Cybersecurity Dimension of Digital Sovereignty

The second dimension of digital sovereignty contributing strongly to strategic autonomy is cybersecurity. In this field, the EU's reliance on Chinese 5G infrastructure has been cited as a serious

[20] https://ecommerce-europe.eu/news-item/european-commission-launches-process-to-adopt-legal-framework-for-eu-us-data-flows/

[21] Putting tech and innovation at the service of people and the green transition | by UCL Institute for Innovation and Public Purpose | UCL IIPP Blog | Medium

problem. The lack of a truly single European cyberspace may in fact leave the EU vulnerable to foreign manipulation. Back in 2019 already, Member States, with the support of the Commission and the European Agency for Cybersecurity (ENISA) published a report[22] on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks. The report warned against over-dependence on one equipment supplier, which increases exposure to potential supply interruption and creates a security risk. Furthermore, the report stressed how cyber-criminals are taking advantage of the coronavirus pandemic, with a dramatic increase in the number of cyber-attacks (Madiega, 2020). On top of over-dependence and supply-chain interruption concerns, the cyber-security dimension is also strictly related to the power play between the US and China and the associated accusation of state-funded cyber-espionage on both sides. This has further drawn the cybersecurity dimension of digital sovereignty into the spotlight (Baischew *et al.* 2020).

In the cybersecurity arena, the EU's approach is not only focusing at fencing off direct attacks and mitigate risks of overdependency and espionage; it also actively pursues transparency and trust. In keeping up with EU values and objectives, the task for the Union is to continue to promote new standards and practices that guarantee that digital services are reliable and controllable, even when they are produced abroad. More specifically, the EU action on cybersecurity is revolving around a few specific areas:

- First, a review of the EU framework for cybersecurity certification program, which offers a uniform set of regulations to guarantee that businesses and consumers are safeguarded in the EU, is due in 2023. While several nations have recently improved their cybersecurity legislation with specific references to the NIS Directive and pertinent EU regulations, establishing a mandatory EU-wide certification scheme (and not just a purely voluntary one as is the case today) would be a step forward in ensuring a truly safe environment, especially for 5G networks. It could also foster the establishment of the EU as a standard-setter in the field of cybersecurity. According to the 5G Public Private Partnership, the establishment of uniform security standards[23] would be a significant step in strengthening Europe's technological know-how and industrial leadership in 5G networks and towards smart connectivity systems. Additionally, the EU might collaborate to establish global standards in the IoT space, where there are still few standards available (there is, in fact, no standard for implementing cybersecurity in smart devices).
- Second, inadequate cooperation in cybersecurity-related subjects has been noted as one of the key problems that EU policymakers need to address. A report from the EU Court of Auditors[24] emphasizes that more EU action is required to address inconsistent transposition or gaps in EU law (such as limited and diverse legal frameworks for duties of care; the EU's company law directives have no specific requirements on the disclosure of cyber risks). This is true even though the establishment of a new Joint Cybersecurity Unit will strengthen the cooperation between the Member States on these topics. Finalizing the adoption of the Commission's proposal to create European Cybersecurity Competence Centers[25] would also be a significant step in the right direction to reinforce the cybersecurity dimension of the EU digital sovereignty.
- Third, a review of EU procurement policies has been triggered by the fear of cybersecurity threats. A European Parliament resolution[26] from 2019 urged for security to be made a requirement in all EU and state public procurement processes for critical infrastructure. Member States should create particular security requirements, including obligatory ones for cybersecurity certification, that might be used in the context of public procurement for 5G networks. In a broader sense, the reworking of the EU's public procurement regulations and grant provisions to better account for the crucial features of digital technologies in delicate industries might be evaluated. That would entail giving

[22] Report on EU coordinated risk assessment of 5G (europa.eu)

[23] Advancing Software Security in the EU — ENISA (europa.eu)

[24] Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper) (europa.eu)

[25] Carriages preview | Legislative Train Schedule (europa.eu)

[26] printsummary.pdf (europa.eu)

security factors more weight when assessing bidding proposals and putting more focus on the diversity of ICT providers as well through the openness of network equipment supply chains. It would also be beneficial in this regard to revise the Directive on Security of Network and Information Systems (NIS Directive)[27] to harmonize the protection of the crucial digital sector within the EU and to complete the adoption of an international procurement instrument[28]. This with the aim of guaranteeing reciprocal market access in public procurement. A framework for cooperative procurement for cybersecurity infrastructure in the EU should also be investigated, according to the EU Court of Auditors[29].

The Strategic and Geo-Political Dimension of Digital Sovereignty

The strategic and geo-political dimension of digital sovereignty has gained significant traction thanks to the renewed assertiveness of the von der Leyen's Commission on the international scene. The EU and its Member States are facing an increasingly complex situation in international relations. The EU will have to adapt to this situation and retain a voice of its own if it does not want to put its ability to act autonomously at risk. The recent developments associated to the Covid-19 pandemic, as well as to the economic instability related to the war in Ukraine have pointed to critical issues in Europe such as the reduced autonomy of crucial national ICT infrastructure and the increased dependency of value chains. This dimension of digital sovereignty is therefore deeply interwoven with the very concept of national and European sovereignty in its most traditional connotation – the supreme authority of a state (or a supra-national entity) over its territory, people, and resources.

A recent paper published by European Parliamentary Research Service (EPRS)[30] draws the link between strategic autonomy and digital sovereignty as it underscores "digital dependence on the USA and China" as the trigger for heightened attention of EU policymakers on gaining digital sovereignty. The Commission's stance on minimizing this technology (digital) dependence is reflected in a number of policy measures with the aim appearing to be centered on (re-)gaining control over data.

A single European Data Space

First and foremost, the European Commission recognises[31] that data is at the centre of the digital transformation and that data is therefore the most fundamental and important building block for the long-term economic growth in Europe. As such, data access and data sharing in Europe becomes a key factor to ensure short-term recovery from the pandemic and counter the economic downturns linked to the war in Ukraine and their related value-chain disruptions and inflationary pressures. Accordingly, one of the first policy initiatives echoing this push towards the provision of digital tools originating in the EU was the plan to create a single European data space. This concept refers to an EU designed single market for data that shall enable companies (and in particular SMEs) across the EU to reap the benefits from data which would otherwise be difficult or impossible for them to access. The European Strategy for Data outlines the concept in detail while commissioner Thierry Breton summarises its goal as follows[32] "European data will be used by European companies […] to create value in Europe."

[27] The NIS Directive | Cyberwatching
[28] Carriages preview | Legislative Train Schedule (europa.eu)
[29] Review No 02/2019: Challenges to effective EU cybersecurity policy (Briefing Paper) (europa.eu)
[30] See EPRS (2020): On the path to 'strategic autonomy' – The EU in an evolving geopolitical environment. European Parliamentary Research Service. PE 652.096.
[31] See Bayer, L. (2019): Meet von der Leyen's 'geopolitical Commission'. Politico. Online article: https://www.politico.eu/article/meet-ursula-von-der-leyen-geopolitical-commission
[32]EC AV PORTAL (europa.eu)

The "AI-Airbus" of the Digital Space: GAIA-X

Another fundamental step to strengthen the EU digital sovereignty on the global stage is the Franco-German project GAIA-X. The initiative aims to establish a common data infrastructure based on European values. Specifically, the German Federal Ministry for Economic Affairs understands "…data infrastructure as a federated technical infrastructure, consisting of components and services that make it possible to access data and to store, exchange and use it according to predefined rules. We understand a digital ecosystem as the network of developers, providers and users of digital products and services, connected with transparency, wide-based access and a vibrant process of interchange. Such a system thus serves as a crucial foundation for European growth, digital innovations and new business models." [33] The central contribution of GAIA-X is a shared 'architecture' for data storage and sharing. "The architecture employs digital processes and information technology to facilitate the interconnection between all participants in the European digital economy. By leveraging existing standards, open technology and concepts, it enables open, consistent, quality-assured and easy-to-use innovative data exchange and services. Additionally, GAIA-X will become a facilitator for interoperability and interconnection between its participants for data as well as services[34] (Baischew *et al*, 2020).

Directly related to GAIA-X and its ability to improve data (re-)use and sharing is artificial intelligence (AI) as a key capability for the EU and its Member States on their long road to international and geopolitical digital sovereignty. The Commission's objective is to support cutting-edge research in AI and its applications in order to realize the economic potential that it offers, in keeping with the strategic aspect of digital sovereignty. To this end, the Commission aims to unify the approach towards AI based on European values, norms and ethics across Member States of which many have already launched their own individual AI strategies[35]. The European High Performance Computing Joint Undertaking is another illustration of current Commission policy measures that are in line with the strategic aspect of digital sovereignty (Euro HPC JU)[36]. It stands for a legislative and financial tool aimed at creating a pan-European supercomputing infrastructure that will be used in a variety of research and commercial application areas, including but not restricted to the creation of AI application. With the European industry only providing around 5 percent of supercomputing resources while consuming approximately 30 percent of these resources[37] (and the difference coming from competitors in the US, China and Japan) the Euro HPC JU aims to build HPCs within the EU alleviating the existing dependency on non-EU computing power[38]. This Joint Undertaking will have a budget of around 1 billion euros with additional resources provided by private entities.

5G Rollout in the EU

Perhaps the topic featuring most prominently in the public debate around the strategic and geo-political connotation of digital sovereignty is the rollout of 5G technology across the Member States. The European Council demanded a coordinated strategy for 5G network cybersecurity[39], noting that these

[33] Quoted from Federal Ministry for Economic Affairs and Energy, & Federal Ministry of Education and Research (n.d.): Project GAIA-X - A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. Executive Summary. Available at: https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executivesummary.pdf?__blob=publicationFile&v=6. Digital Sovereignty in Europe

[34] Quoted from GAIA-X (2020): GAIA-X Technical Architecture. Available at: https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Publications/gaia-x-technical architecture.pdf?__blob=publicationFile&v=5

[35] https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

[36] See https://eurohpc-ju.europa.eu/ Notably, while the HPC facilities themselves may alleviate the dependency of EU-based enterprises and researchers on non-EU HPC computing power, the vendors selected for projects under the initiative include also non-EU vendors such as Hewlett-Packard Enterprise for a significant number of facilities announced so far.

[37] https://www.eib.org/attachments/pj/financing_the_future_of_supercomputing_en.pdf

[39] EU Recommendation 2019/534, see also https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_1833. 31.

networks face more serious security concerns than earlier network generations. Since a so-called toolbox has been made accessible, Member States must conduct their national risk assessments and collaborate at the European level.

The ensuing debate centered on whether non-EU providers will be permitted to supply the infrastructure necessary for modernizing the corresponding mobile network. In particular, Huawei and ZTE – the Chinese competitors of the European suppliers Ericsson and Nokia – have drawn the attention of policymakers and regulators throughout the EU as well as in the UK. Various countries have decided to (partly) exclude Huawei and ZTE from 5G rollout or have set limits for their involvement. It is interesting to note that the publicly stated rationale behind such (partial) bans of non-EU suppliers referred primarily to cybersecurity concerns. The underlying rationale however appears to be much more driven by geopolitics and essentially strategic concerns (Rühlig and Björk, 2020). These EU-level efforts serve as an example of the Commission's goal of (re-)acquiring strategic autonomy with regard to important digital technologies.

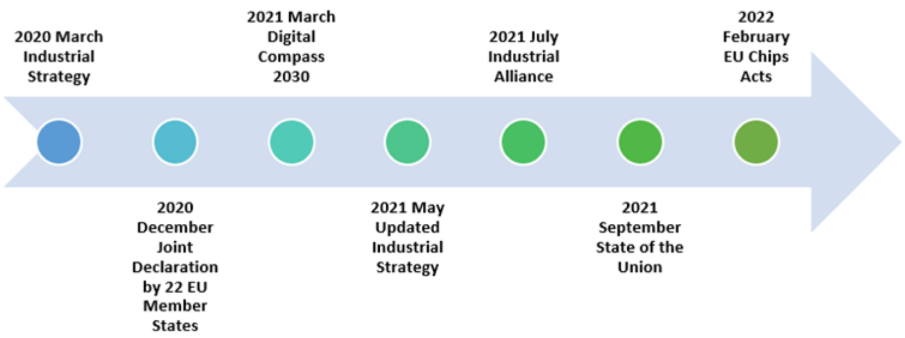
Value Chains Interdependence and Structural Vulnerabilities – The Chips Act

The COVID-19 crisis and its impact on the global and EU economy helped putting the spotlight on another key element of the strategic and geo-political dimension of digital sovereignty – value chains interdependence and structural vulnerabilities in the ICT industry. The day before the WHO officially declared COVID19 a global pandemic, the Commission presented its Industrial Strategy[40] to support the twin transition to a green and digital economy. The strategy a year later was updated[41] to limit Europe's dependencies in key strategic areas and strengthen the resilience of the Single Market. One of the key strategic areas identified in the Staff Working document[42] were the processors and the semiconductor technologies. Microchips and semiconductors are fundamental building blocks of digital products, and the accelerated pace of digital transformations, combined with the sudden shift to working from home, has resulted in a global semiconductor shortage[43]. This affected various industries, however it hit hardly Europe's most important sector, automotive.

Semiconductors are primarily produced in Asia, more specifically in Taiwan (TSMC[44]) which is the biggest global exporter of microprocessors and SoCs designed by US companies, followed by South Korea (Samsung) with 17.1% global market share[45]. Microprocessors, GPUs, SoCs, AI, and memory semiconductors are at the center of strong geostrategic interest. Especially for China and the US that are competing to gain dominance in each sector. Europe responded by enforcing its political narrative of digital sovereignty (also called resilience or strategic autonomy) under which the EU does not necessarily mean protectionism but having the capability to make decisions to better defend European interests and values[46]. Commissioner Thierry Breton emphasized many times in his public speeches that without an autonomous European capacity on microelectronics, there will be no European digital sovereignty; data, microelectronics, and connectivity are the cornerstones of Europe's digital sovereignty[47].

[40] European industrial strategy | European Commission (europa.eu)
[41] Updating the 2020 Industrial Strategy (europa.eu)
[42] SWD on Strategic dependencies and capacities, SWD(2021)
[43] Why is there a shortage of semiconductors? | The Economist
[44] TMSC has 53% share of the global semiconductor foundry market. Source: SWD(2022) 147 final
[45] Ibidem
[46] Digital sovereignty is central to European strategic autonomy – Speech by President Charles Michel at "Masters of digital 2021" online event - PubAffairs Bruxelles
[47] Speech by Commissioner Thierry Breton at Hannover Messe (europa.eu)

Overview of EU's Semiconductor Policy


2020 March Industrial Strategy
2020 December Joint Declaration by 22 EU Member States
2021 March Digital Compass 2030
2021 May Updated Industrial Strategy
2021 July Industrial Alliance
2021 September State of the Union
2022 February EU Chips Acts

The Commission took immediate steps to address the challenge faced by the shortage of these components. Among one of the first steps was the launch of the Industrial Alliance on Processors and Semiconductor technologies[48] with the overall objective to identify the existing gaps and the technology developments necessary for companies and research and technology organisations active in the sector in the EU to be competitive. The alliance brings together various stakeholders, business, academia, research organisations and Member State representatives.

The Commission did further set up a Digital Compass to translate the EUs digital ambitions for 2030 into concrete targets. The objectives are focusing on four cardinal points to map the EU's destination for 2030: a digitally skilled population and highly skilled digital professionals, secure and performant sustainable digital infrastructures, digital transformation of businesses and digitalization of public services. One of the major goals outlined in the 2030 vision is that European semiconductor production, including processor production, should account for at least 20% of global semiconductor production in value, up from 10% in 2020. In February 2022, the EU unveiled a comprehensive set of measures to strengthen the EU's semiconductor ecosystem with the **European Chips Act package**. The package includes a Communication on a Chips Acts for Europe[49] which spells out the European Chips Strategy. Two proposals for a Regulation: a proposal for a Council Regulation establishing the Joint Undertakings under Horizon Europe[50]; and a proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (the Chips Act)[51] and a Recommendation addressing the Member States on a common Union toolbox to address semiconductor shortages and an EU mechanism for monitoring the semiconductor ecosystem[52].

The Chips Act aims to carry out the political commitment made by President von der Leyen, who stated in her State of the Union address[53] in 2021 that the goal is to jointly create a cutting-edge European chip ecosystem, including production in Europe; if adopted it will be directly applicable across all the EU Member States. As a first outcome of the EU Chips Package, the coordination efforts in line with the Recommendation have started and a new public consultation[54] was launched by the Commission addressing the suppliers and the end-users of semiconductors in Europe.

[48] Alliance on Processors and Semiconductor technologies | Shaping Europe's digital future (europa.eu)
[49] EUR-Lex - 52022DC0045 - EN - EUR-Lex (europa.eu)
[50] EUR-Lex - 52022PC0047 - EN - EUR-Lex (europa.eu)
[51] Proposal for a Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) EUR-Lex - 52022PC0046 - EN - EUR-Lex (europa.eu)
[52] EUR-Lex - 32022H0210 - EN - EUR-Lex (europa.eu)
[53] State of the Union Address by President von der Leyen (europa.eu)
[54] European semiconductor value chain consultation | Shaping Europe's digital future (europa.eu)

The initiatives of the European Commission around the European Chips Act point also to another constitutive element of the digital sovereignty's strategic and geopolitical dimension – the need for the EU to acquire considerable computing power. In its intervention in September 2020, Commissioner Breton emphasized the need for Europe to improve its capacity to develop and produce "the most powerful processors, including quantum ones"[55]. The race for an increased production in Europe of semiconductors, as well as the access to the rare earth and the other necessary material for their production, becomes therefore of vital importance for the EU digital sovereignty as these microelectronic components underpin most of the key value chains of the future: cars and connected devices, tablets and smartphones, supercomputers and edge computers, artificial intelligence and defence.

Digital Sovereignty: What it means for the Business Sector

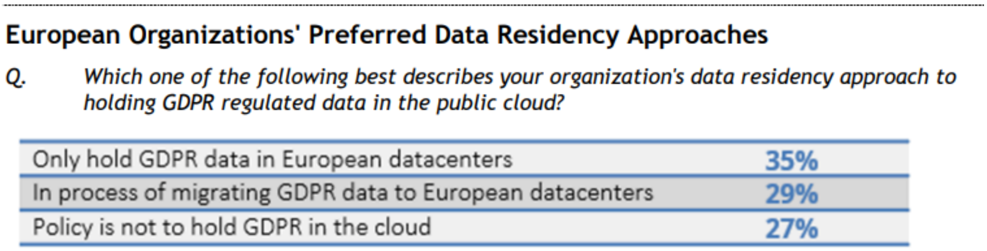
The initiatives taken at EU level under the three dimensions of digital sovereignty are clearly impacting the business sector. The growing extraterritorial application of data governance laws is subjecting organisations to an increasing tension between enabling digital innovation associated with cloud and ensuring that data and IT infrastructures are compliant with regulations and guidelines. When dealing with on-premises infrastructures, the data sovereignty principles set out by the EU are clear cut. However, they become a more complex issue when it comes to storing and processing data in the cloud. Much of the conversation around data sovereignty in Europe centers on two main aspects.

- First, extent to which foreign government and law enforcement can legitimately access and request customer data stored extraterritorially. A common misconception about the Clarifying Lawful Overseas Use of Data (CLOUD) Act is that it enables U.S. law enforcement agencies to extract data directly from systems. Only in limited circumstances, and with a judicial mandate, can such authorities request electronic evidence from service providers, even if it is held outside the U.S., thus leaving the data dimension of data sovereignty substantially intact.
- Second, there is the extraterritorial reach of foreign intelligence and surveillance programs authorized under national security laws as well as the level of protection afforded to individuals' privacy, either in country or once their data is transferred to another country. The 2020 Schrems II decision, which invalidates the EU-U.S. Privacy Shield framework, and its focus on U.S. government surveillance laws has left many organisations grappling with whether they can legally and safely transfer data outside the EU, particularly to the U.S. The compliance fallout from the Schrems II decision is pushing a Eurocentric approach to data governance.

As a result of the above - and given the complexity of making risk assessments on third-country laws and practices and the need for additional technical safeguards - data localization is often the only practical option for businesses. It is not surprising therefore that 64% of organisations polled for an IDC survey cited adopting a risk mitigation approach to either holding or migrating GDPR-governed data to datacenters in Europe while around 42% of European organisations opted to undertake greater due diligence of their cloud service providers to determine local hosting capabilities and the adequacy of their legal, privacy, and security safeguards[56].

[55] https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-keys-sovereignty_en

[56] Sovereign Clouds and the Digital Sovereignty Imperative: Europe's Quest for Digital Independence, Market Perspective, IDC, May 2022



European Organizations' Preferred Data Residency Approaches

Q. Which one of the following best describes your organization's data residency approach to holding GDPR regulated data in the public cloud?

Only hold GDPR data in European datacenters	35%
In process of migrating GDPR data to European datacenters	29%
Policy is not to hold GDPR in the cloud	27%

Source: IDC's *European Security Survey*, 2021 (n = 700)

As a consequence of the EU regulatory pressure, organisations in Europe and elsewhere are changing their cloud strategy and turning towards *sovereign cloud*. Savvier enterprise users are becoming aware that all clouds are not the same; those in regulated industries recognize that the right data must be deployed to the right cloud/venue. This results in a multicloud or hybrid IT scenario, with organisations already identifying the best locations for their workloads and applications. Enterprise users that have a less mature approach to digital transformation and cloud are likely to need greater guidance from their business partners and IT consultants as the concept of “trusted cloud” – often used by a number of IT vendors - does not automatically mean a "sovereign" cloud.

However, digital sovereignty is about more than just data. Besides cloud platforms, it also includes workload software, datacenter assets, and communications infrastructure. More importantly, it also encompasses processes and operations used to control and manage infrastructure and digital services. All this covers the entire digital architecture that underpins a digital-first Europe. But while there are rules already in place within the EU about data, the situation with infrastructure or other operational elements associated with digital sovereignty is more fluid. While the Digital Market Act and the Data Governance Act proposed by the European Commission may provide some guidance, European organisations still face uncertainties with infrastructure, especially when it comes to ownership, control, interoperability, and portability at the workload level. For processes, organisations are concerned about the degree of control they have, and the stability of these processes in the long term. Furthermore, there are worries about potential unauthorized access from law enforcement agencies, cloud service providers, and other infrastructure players.

The adoption of third-party public cloud services and data services by European organisations is therefore becoming inseparably connected to their own digital strategies. The broader and more strategic approach to digital sovereignty and the application of its principles can help organisations build greater trust among stakeholders and add business and operational value.

- At the initial stage, the basic application of the traditional data sovereignty concept aims to tightly control compliance with data residency, data protection, cybersecurity, and a European approach to AI.
- At the intermediate stage, data sovereignty improves interoperability and resilience of services by preventing lock-in with a single global provider (or at least enables organisations to make a credible threat to switch). This aims to push providers to deliver the best value for money and innovation. Data and operational resilience can help organisations create a framework to prepare for new and upcoming regulations such as the EU's proposed Digital Operational Resilience Act (DORA), and the U.K.'s Financial Conduct Authority and Bank of England Operational Resilience Rules.
- At the most strategic stage, end-user organisations can maximize opportunities to safely exchange data across enterprises and industries to prompt European-led innovation. The ultimate ambition here is to boost the continent's digital economy, create new jobs, and develop platforms, products and services that enable Europe to better compete on the global digital stage.

In September 2021, IDC surveyed[57] 430 technology leaders across all industries in eight European countries in Western Europe and Central & Eastern Europe and examined the impact of government sustainable initiatives, which relates to national sustainability plans, regulations, and policies set in place to achieve sustainability goals. This first EMEA Future Enterprise Resiliency and Spending (FERS) Survey revealed, interestingly that 69% of organisations in Europe agree that digital sovereignty enhances customer, partner, and government trust in their companies and strengthen company resiliency. Some organisations are already exploring how they can turn their sovereignty-focused strategies into a competitive differentiator. They are actively evaluating the proportion of data and workloads that will need special handling and are setting aside a portion of IT budgets to review and revise their governance frameworks, data, processes, and infrastructure strategies.

DIGITAL SOVEREIGNTY AND ITS STAKEHOLDERS – INITIAL VIEWS

The chapters above present the current state of digital sovereignty in Europe in various dimensions. As mentioned in the methodology section our research team has conducted interviews with stakeholders coming from academia, think tank, private sector, research institute and trade association. In this chapter we will focus on the stakeholders' views and continue the analysis of the concept of digital sovereignty within the **three dimensions of privacy, cybersecurity and geopolitics**.

Table 2 Digital Sovereignty – Key Definitions according to the interviewed stakeholders

Organisation	Definition and reflection on the term of Digital Sovereignty
Trade Association	"At its core, digital sovereignty is the possibility of independent digital self-determination. In an international context, this means above all own design and maintaining scope for innovation and avoiding one-sided dependencies[58]".
Research Institute / Think Tank / Academia	"Digital Sovereignty is not just a question of competitiveness, but also of the political autonomy of the European Union and its member states, the innovativeness of businesses, and the freedom of research institutions and all Europeans in the digital world[59]".
Private Sector	"Be sovereign and still open[60]" / "We recognize that European governments are regulating technology and we will adapt to and support these effort[61]".

Privacy sovereignty for the individual

On 25th May 2018, the EU General Data Protection Regulation (GDPR), which regulates how personal data of EU citizens may be handled and transmitted, came into force. It was a key achievement for the European lawmakers and its was a key achievement also on the international and global front of privacy

[57] Wave 8 of IDC's European FERS Survey (conducted September 1–15, 2021) https://www.idc.com/getdoc.jsp?containerId=EUR148296421

[58] Digitale Souveränität (bitkom.org) Unofficial translation from German

[59] Digital Sovereignty. Status Quo and Perspectives - acatech - National Academy of Science and Engineering

[60] Quote from the interview

[61] Microsoft responds to European Cloud Provider feedback with new programs and principles - EU Policy Blog

legislations. The GDPR is a comprehensive privacy law that is applicable to businesses of all sizes and across all industries. Applicable to all organisations managing European citizen data all over the world.

The GDPR gives a basis for privacy regulations for European citizens. An Austrian student while being in the US and attending university courses on privacy realised how the Big Tech companies, especially Facebook are not aware of the European regulation. That is where the story of a now well-known activist, Maximilian Schrems' started. The first case Schrems has filed against Facebook was on the use of transferring personal data to its headquarters to the US. He argued that this data could be accessed by US intelligence services and in violation of the GDPR.

The story of Maximilian Scherms demonstrates that the importance of the privacy of the individual is not only a matter for regulators but also for citizens in Europe.

During the interview process the aspect of privacy and research came up repeatedly. From the one hand, it is clearly recognized that Europe is a rule setter in the privacy policy front, however on the other hand privacy regulations can set up unforeseeable barriers to other activities such as research and innovation. Storing and keeping data in Europe become a priority, however finding solutions to switch from non-European providers to Europe providers is the biggest challenge academia is facing right now. In this respect, research centres and universities pointed to the difficulty of conducting research on a global level while hosting their research data at their own premises in Europe.

Cybersecurity dimension of the data sharing

The debate in Europe about the term of digital / technological or in some cases cyber sovereignty has been evolving in recent years. Cybersecurity and digital sovereignty are correlated. There is no doubt that one cannot gain independence without infrastructure and technological readiness to respond to potential threats and attacks. Cyber defence is a key element towards reaching Europe's full digital sovereignty. With the recently presented EU Cyber Defence policy and an Action Plan on Military Mobility 2.0[62] the EU aims boosting cooperation and investments in cyber defence to better protect, detect, deter, and defend against a growing number of cyber-attacks.

Stakeholder engagement and support is crucial to fulfil and jointly combat the war in cyberspace. In this respect, DIGITALEUROPE, the biggest European trade association representing the leading digital technology players, has set up a dedicated Executive Council to address the increasing number and the changing nature of digital threats in the new geopolitical context[63]. According to DIGITALEUROPE the public and private sectors need to work closely for a more ambitious EU Cyber Defence Policy in the new European security context. The international community needs to engage more. If nation states, international business, and specialists do not improve international cooperation on cybersecurity definitions and solutions, the global digital economy runs the risk of becoming more and more vulnerable to cyberattacks[64].

The Strategic and Geo-Political Dimension of Digital Sovereignty

On the day when the Data Governance Act was officially presented to the public. Commissioner of Internal Market, Thierry Breton, used the following words:

"We are defining today a truly European approach to data sharing. Our new regulation will enable trust and facilitate the flow of data across sectors and Member States while putting all those who generate data in the driving seat. With the ever-growing role of industrial data in our economy**, Europe needs**

[62] Cyber Defence: EU boosts action against cyber threats (europa.eu)
[63] DIGITALEUROPEs-recommendations-for-a-more-ambitious-EU-Cyber-Defence-Policy_.pdf (digital-europe-website-v1.s3.fr-par.scw.cloud)
[64] Ibidem

an open yet sovereign Single Market for data. Flanked by the right investments and key infrastructures, our regulation will help Europe become the world's number one data continent[65]."

The emphasis is therefore on the open yet sovereign Single Market for data, where Europe aims to succeed by its rules and regulations and yet again set up the standards for the rest of the world. Surprising as it may seem, some key tech actors decided to listen to the needs of European leaders and instead of trying to get into lengthy judicial disputes propose a solution that would work for all the parties involved. We can find many sources on how the Big Tech defines digital sovereignty, in this paper we share the view of Microsoft Corporation. The multinational tech giant highlighted that **sovereignty can and should go be open**. This view is demonstrated by the company's announcement of the EU Data Boundary for the Microsoft Cloud from 1 January 2023[66]. According to the announcement Microsoft offers the possibility for public sector and commercial customers in the EU and EFTA to store and process all their costumer's data in Europe by the end of 2022.

[65] Commission proposes measures to boost data sharing (europa.eu)

[66] Microsoft announces the phased rollout of the EU Data Boundary for the Microsoft Cloud begins January 1, 2023 - EU Policy Blog

CONCLUSIONS AND POLICY IMPLICATIONS

The notion of digital sovereignty is not new in the academic and political debate. With the rapid emergence and consolidation of a digital economy in Europe and elsewhere, supra-national institutions, individual countries, businesses and industry representatives have indeed pointed to the increased necessity to act independently and autonomously in the digital domain. However, It is only with the advent of the Von der Leyen Commission that digital sovereignty has found a stable and prominent position in the EU political agenda – in terms of programmatic claim, as well as through specific policy measures and practical implementations.

This story has provided a comprehensive overview of the concept of digital sovereignty in Europe and has highlighted some of the principal initiatives undertaken at the EU level to make Europe digitally sovereign. To do so, it has adopted a three-dimensional analytical framework built on concrete policy directions: a) the privacy and data protection dimension of digital sovereignty axed on the ability for European organisations and citizens to control their own data and digital lives; b) the cybersecurity dimension of digital sovereignty centered on the need to promote a unified and effective cyberspace to counter Europe's digital structure overdependence on few and non-European technology providers; c) the strategic/geopolitical dimension of digital sovereignty with the aim to promote a European alternative to the EU's economic and ideological rivals in the digital space at global level.

The adoption of on such empirical definition, operationalized along these three dimensions, has had the merit to tackle the ambiguity that still surrounds the notion of digital sovereignty. Additional concepts such as the development of R&D competencies and digital skills, the preservation of leadership positions in key digital technologies, or the ability to safeguard EU's strategic autonomy, have therefore been captured by the privacy and data protection, the cybersecurity and the strategic/geo-political framework.

The primary research effort conducted with trade and industry associations, research institutes, think tanks and academia, as well as the private sector, has highlighted – not surprisingly – that digital sovereignty as such is not univocally understood. While advocating for a more pronounced independent digital self-determination, trade associations and industry representatives, for example, tend to highlight the need for Europe to maintain innovation potential without cutting fundamental cooperation exchanges with other players on the global stage. Research and academia, on the other hand, insist on the need to achieve political and economic autonomy in the EU and at Member State level vis-à-vis Europe's partners or competitors. The private sector welcomes a regulatory stance by national and EU institutions provided that this interventionist approach does not undermine Europe's capacity to remain open, competitive and able to innovate. On top of these different views on digital sovereignty by multiple stakeholders, Member States too appear to have different positions vis-à-vis digital sovereignty initiatives. Countries like France and Germany have demonstrated to appreciate the design and implementation of prescriptive policies and have fruitfully initiated a close collaboration around different themes with the GAIA-X project on the forefront. Other Member States (often smaller Member States with more open economies) see potential risks linked to a top-down approach to digital sovereignty imposed at the EU level. Deprived as they are of a strong technology industry, their access to cutting-edge digital developments, new economic opportunities and productive partnerships with non-EU members could in fact become more problematic.

Despite these apparent challenges, the European Commission is successfully pursing its efforts towards a more digitally sovereign Europe along the lines of the EU Digital Strategy and the European Strategy for Data. Going forward, a rationalization of these initiatives into a more coherent lot and a clear prioritization of these interventions along a set of shared criteria of urgency and importance could help the vast variety of stakeholders involved in digital policies to engage more fruitfully along the path of digital sovereignty in the EU.

BIBLIOGRAPHY AND REFERENCES

Assemblée Nationale (2021). Rapports d'information XVe Législature - Législature courante - Mission d'information sur le thème « Bâtir et promouvoir une souveraineté numérique nationale et européenne » - N° 4299 Tome 1 29 juin 2021

Baischew, D.; Kroon, P.; Lucidi, S.; Maerkel, Ch.; Soerries, B. (2020). Digital Sovereignty in Europe – A first Benchmark, WIK Consult, Report, December 2020

Bauer, M., Erixon, F. (2020). Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls. ECIPE occasional paper, 02/2020

Bellanger, P. (2012). De la souveraineté numérique. Dans *Le Débat* 2012/3 (n° 170), pages 149 à 159

Benhamou, B. (2017). Les dimensions internationales de la souveraineté numérique, Dans *Les Nouveaux Cahiers du Conseil constitutionnel* 2017/4 (N° 57), pages 87 à 99

BITKOM (2019). Digitale Souveränität: Anforderungen an Technologien und Kompetenzfelder mit Schlüsselfunktion – Stellungnahme, Bitkom e.V. - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V, 2019 https://www.bitkom.org/sites/main/files/2020-01/200116_stellungnahme_digitale-souveranitat.pdf

Blandin, A. (2016). *Droits et souveraineté numérique en Europe*, Bruylant.

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

Bundesministerium für Wirtschaft und Energie (BMWi) (2021) Schwerpunktstudie Digitale Souveränität Bestandsaufnahme und Handlungsfelder. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.pdf?__blob=publicationFile&v=6

Calderaro, A. (2020). Overcoming fragmentation in cyber diplomacy: the promise of cyber capacity building. [Online]. ISPI. Available at: https://www.ispionline.it/it/pubblicazione/overcoming-fragmentation-cyber-diplomacy-promise-cyber-capacity-building-25418

Couture, S. and Toupin, S. (2018). What Does the Concept of 'Sovereignty' Mean in Digital, Network and Technological Sovereignty? (January 22, 2018). GigaNet: *Global Internet Governance Academic Network, Annual Symposium 2017*, Available at SSRN: https://ssrn.com/abstract=3107272 or http://dx.doi.org/10.2139/ssrn.3107272

Couture, S. and Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital?
First Published August 12, 2019 Review Article Volume: 21 issue: 10, page(s): 2305-2322
https://doi.org/10.1177/1461444819865984

Crespi, F., Caravella, S., Menghini, M., Salvatori, C. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy", Intereconomics, vol. 6, Nov-Dec. 2021: European Commission, *Key Enabling Technologies for Europe's technological Sovereignty*, Brussels 2021

The Economist (2020). *Special report: The data economy*, The Economist, February 22nd,2020 https://www.economist.com/special-report/2020-02-22

European Commission (2019). European Political Strategy Centre, Rethinking strategic autonomy in the digital age, Publications Office, 2019, https://data.europa.eu/doi/10.2872/231231

European Commission (2020a). Making Europe's businesses future-ready: A new industrial strategy for a globally competitive, green and digital Europe. Luxembourg: Office for Official Publications of the European Communities.

European Commission (2020b). A European strategy for data (COM(2020) 66 final). Luxembourg: Office for Official Publications of the European Communities.

European Commission (2020c). Shaping Europe's digital future. Luxembourg: Office for Official Publications of the European Communities.

European Commission (2020d). Towards a European strategy on business-to-government data sharing for the public interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing. Luxembourg: Office for Official Publications of the European Communities.

European Commission (2020e). Proposal for a Regulation on European data governance (Data Governance Act) (COM/2020/767 final). Luxembourg: Office for Official Publications of the European Communities.

European Commission (2020f). Proposal for a Regulation on a Single Market For Digital Services (Digital Services Act) (COM/2020/825 final). Luxembourg: Office for Official Publications of the European Communities

European Commission (2021b)., Proposal for a Decision establishing the 2030 Policy Programme "Path to the Digital Decade" COM(2021) 574 final; European Commission "Shaping Europe's Digital Future" https://ec.europa.eu/info/sites/default/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf

European Economic and Social Committee (2020). The digital single market - trends and opportunities for SMEs (own-initiative opinion), published on 18 September 2020, https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/digital-single-market-trends-and-opportunities-smes-own-initiative-opinion

European Parliament (2021). A European strategy for data, 2020/2217(INI) - 25/03/2021 - Text adopted by Parliament, single reading, Legislative Observatory, 2021 https://oeil.secure.europarl.europa.eu/oeil/popups/summary.do?id=1656816&t=d&l=en

European Political Strategy Centre (EPSC, 2019). Rethinking Strategic Autonomy in the Digital Age, Issue 30, 18 July 2019

Floridi, L. (2019). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Published online, 12 August 2019, Springer Nature h.v. 2020

Frankfuerter Allgemeine Zeitung (2020). ‚Die EU zieht in die Datenschlacht'. Frankfuerter Allgemeine Zeitung, 18.11.2020 https://www.faz.net/aktuell/wirtschaft/wie-die-datenstrategie-der-eu-aussieht-17057357.html

Friedrichsen, M., Peter, J. (2016). *Digitale Souveränität - Vertrauen in der Netzwerkgesellschaft*, Springer, 2016

Glasze, G., Odzuck, E., Staples, R. (2021). Was heißt digitale Souveränität? Diskurse, Praktiken und Voraussetzungen »individueller« und »staatlicher Souveränität« im digitalen Zeitalter", Interner EFI-Workshop 14.06.2021 Sammelbandprojekt, 14.06.2021

Gräf, E., Lahmann, H. , Otto, Ph. (2018). Die Stärkung der digitalen Souveränität - Wege der Annäherung an ein Ideal im Wandel, Deutsches Institut für Vertrauen und Sicherheit im Internet – DIVSI, 2018

Gueham, F. (2017). *Vers la souveraineté numérique*, Fondation pour l'innovation politique, January 2017

Halpin, H. (2008). La souveraineté numérique - L'aristocratie immatérielle du World Wide Web Dans *Multitudes* 2008/4 (n° 35), pages 201 à 213

Lippert, B., von Ondarza, N., Perthes, V. (Hg.), (2019). Strategische Autonomie Europas: Akteure, Handlungsfelder, Zielkonflikte. Stiftung Wissenschaft und Politik, SWP-Studie 2019/S 02, 01.02.2019, 44 Seiten
doi:10.18449/2019S02

Kalff, D; Renda, A.(2019). Mapping Europe's sources of competitive advantage in doing business. Centre for European Policy Studies (CEPS), Brussels, 2019

Komaitis, K. (2021). Europe's ambition for digital sovereignty must not undermine the internet's values. Computer Fraud & Security, 2021(1), 11–13. https://doi.org/10.1016/S1361-3723(21)00008-7

Kuo, L. (2022). Plan Calcul: France's National Information Technology Ambition and Instrument of National Independence. *Business History Review*, 1-25. doi:10.1017/S0007680521000441

Krasner, D.B. (2001). *Problematic sovereignty: Contested rules and political possibilities*, Columbia University Press.

Madiega, T. (2020). "Digital sovereignty for Europe", EPRS Ideas Paper, Towards a more resilient EU, EPRS, European Parliamentary Research Service, PE 651.992 - July 2020

Mannoni, S., Stazi, G. (2021). *Sovranità.com. Potere pubblico e privato ai tempi del cyberspazio*. Editoriale Scientifica, 2021

Massaro, M. (2019). Between Integration and Protection of National Sovereignty in the European Union's Radio Sp'ectrum Policy: Uncovering Potential Research Avenues. *Journal of Information Policy*, 2019, Vol 9 (2019), pp.174-213, Penn State University Press.

McKinsey & Company (2017). Shaping the future of work in Europe's digital front-runners - Digitally-enabled automation and artificial intelligence, October 2017 https://www.mckinsey.com/~/media/mckinsey/featured%20insights/europe/shaping%20the%20future%20of%20work%20in%20europes%20nine%20digital%20front%20runner%20countries/shaping-the-future-of-work-in-europes-digital-front-runners.ashx

McKinsey & Company (2020). Shaping the digital transformation in Europe, Working Paper – Economic Potential. file:///C:/Users/gmicheletti/Downloads/20200218_-_economic_potential_summary_paper_9E3D97F4-BF12-1422-0EA7680FAAE60617_64962.pdf

Moerel, E.M.L. and Timmers, (2021), Reflections on Digital Sovereignty (January 2021). *EU Cyber Direct, Research in Focus series* 2021, Available at SSRN: https://ssrn.com/abstract=3772777

Obendiek, A. S. (2022). Take back control? digital sovereignty and a vision for europe (Ser. Jacques delors centre / policy papers). Hertie School. Retrieved 2023

OECD (2020). Digital Transformation in the Age of COVID-19: Building Resilience and Bridging Divides, Digital Economy Outlook 2020 Supplement. OECD, Paris www.oecd.org/digital/digital-economy-outlook-covid.pdf.

Perarnaud, C. (2021). A step back to look ahead: mapping coalitions on data flows and platform regulation in the Council of the EU (2016-2019). *Internet Policy Review*, 10(2). https://doi.org/10.14763/2021.2.156

Perarnaud, C. (2022). Power to the connected? Determinants of member states' bargaining success in the making of the EU Digital Single Market, *Journal of Cyber Policy*, DOI: 10.1080/23738871.2022.20303

Perarnaud, C and Fanni, R. (2022). The EU Data Act: Towards a new European data revolution? CEPS Policy Insights No 2022-05. March 2022

Pohle, J. (2020). Digitale Souveränität in: *Handbuch Digitalisierung in Staat und Verwaltung*, pp 241-253, Springer, 2020

Pohle, J. and Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1532

Polito, C. (2021). *La governance globale dei dati e la sovranità digitale europea*, IAI-Istituto Affari Internazionali

Présidence française du Conseil de l'Union européenne (2021) : Relance, puissance, appartenance - Le programme de la présidence française du Conseil de l'Union européenne https://presidence-francaise.consilium.europa.eu/media/zeqny1y5/fr_programme-pfue-v2-5.pdf

RamahandryBonneau Bani,Vlasov, Flickenschild, Batura, Tcholtchev, Lämmel, Boerger, (2021) Key enabling technologies for Europe's technological sovereignty. STUDY Panel for the Future of Science and Technology EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 697.184 – December 2021

Renda, A. (2022). 'Leveraging Digital Regulation for Strategic Autonomy'. FEPS, Policy Brief, March 2022 https://www.feps-europe.eu/attachments/publications/220301%20beyond%20the%20brussels%20effect.pdf

Rhinard, M.; Stoestedt, G. (2019). The EU as a Global Actor: A new conceptualization four decades after 'actorness'. *U-Paper*, 6/2019, The Swedish Institute of International Affairs.

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M. and Floridi, L., Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies (October 6, 2021). *Internet Policy Review*, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3937345 or http://dx.doi.org/10.2139/ssrn.3937345

Rühlig, T. & Björk, M. (2020): What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe. Stockholm: The Swedish Institute of International Affairs

Sénat de la République (2019). Le devoir de souveraineté numérique (rapport de commission d'enquête), Rapport n° 7 (2019-2020) de M. Gérard LONGUET, fait au nom de la commission d'enquête, déposé le 1er octobre 2019

Scott Marcus, J., Petropoulos, G., Yeung, T. (2019). Contribution to Growth: The European Digital Single Market Delivering economic benefits for citizens and businesses, Bruegel. (10.1017/err.2017.9)

Soete, L. (2005). "On the dynamics of innovation policy: A Dutch perspective," in De Gijsel, P. and Schenk, H. (eds.), *Multidisciplinary Economics*. Dordrecht, (Springer), 2005.

Soete, L. (2007). From Industrial to Innovation Policy. *J Ind Compet Trade* 7, 273 (2007). https://doi.org/10.1007/s10842-007-0019-5

Steiner, F. und Grzymek, V. (2020). Digitale Souveränität in der EU, Vision Europe | Juli 2020

Timmers, P. (2022). 'Strategic Autonomy Tech Alliances: Political-Industrial Collaboration in Strategic Technologies', FEPS Policy Brief, April 2022 https://www.feps-europe.eu/attachments/publications/220331%20final_strategic%20autonomy%20tech%20alliances-3a.pdf

Türk, P. (2020). Définition et enjeux de la souveraineté numérique. https://www.vie-publique.fr/parole-d'expert/276125-definition-et-enjeux-de-la-souverainete-numerique

Wittpahl, V. (2020). Digitale Souveränität - Bürger | Unternehmen | Staat, Institut für Innovation und Technik (iit), Springer, 2020

Zuboff, S. (2019). The age of surveillance capitalism : the fight for a human future at the new frontier of power (First). PublicAffairs

IDC Sources

- The New Norm: Digital Sovereignty — Policy and Spending Impact (idc.com)
- Cloud Trends in Europe — 2022 Predictions (idc.com)
- IDC FutureScape: Worldwide IT Industry 2022 Predictions
- What are the Benefits of Using Local, as Opposed to Global, Cloud Providers? (idc.com)

Other

1. Digital sovereignty for Europe (europa.eu)
2. The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf (atlanticcouncil.org)
3. Strengthening Europe's digital and technological sovereignty - EU2020 - EN
4. Digital Sovereignty, European Strength and the Data and Cloud Economy – in varietate concordia - Groupe d'études géopolitiques (geopolitique.eu)
5. Who owns data and who controls it? | World Economic Forum (weforum.org)
6. Digital sovereignty for Europe (europa.eu)
7. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf
8. https://www.weforum.org/agenda/2021/03/europe-digital-sovereignty/
9. https://policyreview.info/pdf/policyreview-2020-4-1532.pdf
10. https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/
11. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9387709
12. https://www.vie-publique.fr/parole-dexpert/276125-definition-et-enjeux-de-la-souverainete-numerique
13. https://www.fondapol.org/etude/farid-gueham-vers-la-souverainete-numerique/