Understanding Digital Sovereignty from the lens of EU legal documents

Siraj Anand[1], Abhishta Abhishta[1], Michel Ehrenhard[1], Lambert J. M. Nieuwenhuis[1]
[1]University of Twente

Abstract

This paper examines the European Union's (EU) concept of digital sovereignty through an analysis of 79 legal documents selected via a rigorous screening process. By evaluating mentions of Digital Sovereignty in these documents, this study identifies four key motivations: increasing foreign digital dependencies, lack of common governance, insufficient security amid rising threats, and the growing social and economic impact of technology. Using Gioia methodology, it recognises six dimensions for EU's strategic goals: data control, democratic digital transformation, open strategic autonomy, a digital single market, building own digital capacities, and enhancing cybersecurity & resilience. Our analysis of EU legal documents offers a systematic interpretation of the term "Digital Sovereignty" by differentiating at policy, organisational, and individual levels, providing guidance towards building resilient telecommunication systems.

1 Introduction

Managing the trade-off between the benefits of emerging information technologies within the economic value chain and the need to ensure the security & resilience of digital infrastructure, poses a significant challenge for businesses as well as for policymakers[Dutta and McCrohan, 2002]. Keeping up with the evolving needs of consumers/citizens is more challenging in economies like the EU, where 90% of data is managed by foreign companies and less than 4% of the top global online platforms are domestic.[1] As digital transformation accelerates, it diminishes the state's control over their digital economy, making it crucial to maintain a degree of oversight and transparency over telecommunication infrastructures and their underlying technologies[Hesselman et al., 2020]. To tackle this challenge, various digital strategies are being discussed to increase trust and security in cyberspace.

The declining security and rising cyber threats to critical infrastructures have led to the emergence of various digital governance models, deeply influenced by the geopolitical and geo-economic dimensions of cyberspace[Bradford, 2023]. Many economies are increasingly adopting interventionist digital policies and strategies to tackle these challenges[Foster and Azmeh, 2019], with expanding regulatory frameworks and compliance guidelines aiming to preserve state sovereignty within the digital landscape. In more recent years, the narrative of digital sovereignty repeats very often European policy, addressing concerns about "digital foreign interference by state actors" and dependence on foreign digital governance laws, platforms, and infrastructures[Jansen et al., 2023; Broeders et al., 2023b]. It is not only viewed as a geopolitical concern but also as a means to develop a secure and resilient society while reducing dependence on other regions Monsees and Lambach [2022]. However, the notion of digital sovereignty being complex and multifaceted is under-defined and has no universally accepted definition.

Although the traditional concept of sovereignty is defined as the capacity to maintain order within a nation-state's territory without external interference, remains largely unchanged in practice[Philpott, 1995; Osiander, 2001; Humphrey, 2007], some countries and organizations advocate for multi-stakeholder governance models. While these models are designed to promote strategic collaboration between businesses and governments, their effectiveness in ensuring market competitiveness and safeguarding sovereignty in cyberspace will benefit from further clarity and understanding of digital sovereignty. Without a clear understanding of digital sovereignty within the broader context of digital governance, future telecommunication technologies (such as Hesselman et al. [2020]) will fall short. Therefore, this article aims to explore EU legal documents, addressing the following research question(RQ):

What does EU mean by digital sovereignty in its legal documents?

[1]Definitive adoption (EU, Euratom) 2024/207 of the European Union's annual budget for the financial year 2024

This study investigates the main research question by addressing the following sub-questions:

SQ1. What is the motivation for digital sovereignty?

SQ2. What are the intended goals of proposing digital sovereignty?

The first question explores the foundational issues and challenges driving the EU's emphasis on digital sovereignty. The second investigates its purpose, relevance, and role in shaping Europe's digital governance and resilience strategies. To this end, we filtered out 248 EU legal documents sourced from the official repository maintained by the publications office of the European Union that addressed digital sovereignty in the text. We select 79 relevant documents for qualitative analysis to investigate the motivation behind the EU's push for digital sovereignty and use Gioia methodology [Gioia et al., 2013] to evaluate its associated goals. We have taken reference from multiple uses of the Gioia method in the literature[Javadian et al., 2020; Leemann and Kanbach, 2022; Fiorito et al., 2023; Ménez-Partearroyo and Rana, 2024] to help us analyse the goals of digital sovereignty.

The rest of the paper is structured as follows, Section 2 reviews the academic and legislative literature on the evolution of digital sovereignty in Europe. Section 3 presents the process of document selection and the methodology. In Section 4, we present and discuss the identified themes for EU's motivation and the dimensions for intended goals. We conclude this study in Section 5 by systematically linking the identified motivations with dimensions of goals to facilitate a clear understanding of digital sovereignty based on EU legal documents.

2 Digital Sovereignty in Europe

In this section, we provide an overview of how the term digital sovereignty is discussed in literature and European policy. We also analyse and compare the trends in documents published in both the literature and EU policy.

2.1 Digital Sovereignty in literature

The discussion on the sovereignty of digital infrastructures began in the late twentieth century, with foundational work by [Grant, 1983; Philpott, 1995] and others. This discussion laid the groundwork for the establishment of the Electronic Frontier Foundation (EFF) in 1996 by John Perry Barlow, who later launched the Declaration on the Independence of Cyberspace, arguing against the notion of borders in cyberspace and the lack of sovereignty in this domain[2]. Since then, the concept of sovereignty in cyberspace has been a constant theme in political, institutional, and academic circles[Lloyd, 1993; Philpott, 1995; Schaller, 2001; Osiander, 2001; Humphrey, 2007; Franzese, 2009].

With increased literature, different groups have different interpretations of digital sovereignty based on their requirements[Couture and Toupin, 2019]. One which considers digital sovereignty merely a digital version of traditional sovereignty principles influenced by political interests, pushing for leadership over global digital landscape[Amoore and de Goede, 2008; Bigo, 2014; Schaake and Vermeulen, 2016; Lambach and Oppermann, 2023]. Others underscore the importance of coordination between businesses and governments in the digital space, particularly concerning critical infrastructures, to ensure a secure economy and a resilient society. They consider that digital sovereignty could play a role in designing solutions in response to the challenges posed by rapid digital transformation in all sectors, fostering innovation in critical digital technologies, interoperability in public sector and evolution of new digital firms [Gruber, 2017; Mueller, 2010; Beica, 2018; Mueller, 2019; Podszun, 2019; Pohle and Thiel, 2020; Chander and Sun, 2021; Musiani, 2022; Bruno et al., 2024]. Nonetheless, both consider it as highly related to the ability of a state or organisation to act independently, making its own decisions in cyberspace while ensuring that businesses can protect their commercial interests and operate within a stable regulatory environment[Leonard et al., 2022; Broeders et al., 2023b; Blancato, 2024b].

Researchers have attempted to understand the concept of *digital sovereignty* using literature and data/findings from the Information Systems, but with the increasing use of the term 'sovereignty' in the academic literature, many similar concepts like data sovereignty[Hummel et al., 2021], technological sovereignty[Seidl and Schmitz, 2023], and cloud sovereignty[Blancato, 2024a] developed. Only a limited number of studies attempted to delimit these terms from digital sovereignty with the review from

[2]Barlow, J. P. (1996). Declaration on the Independence of Cyberspace. https://www.eff.org/cyberspace-independence

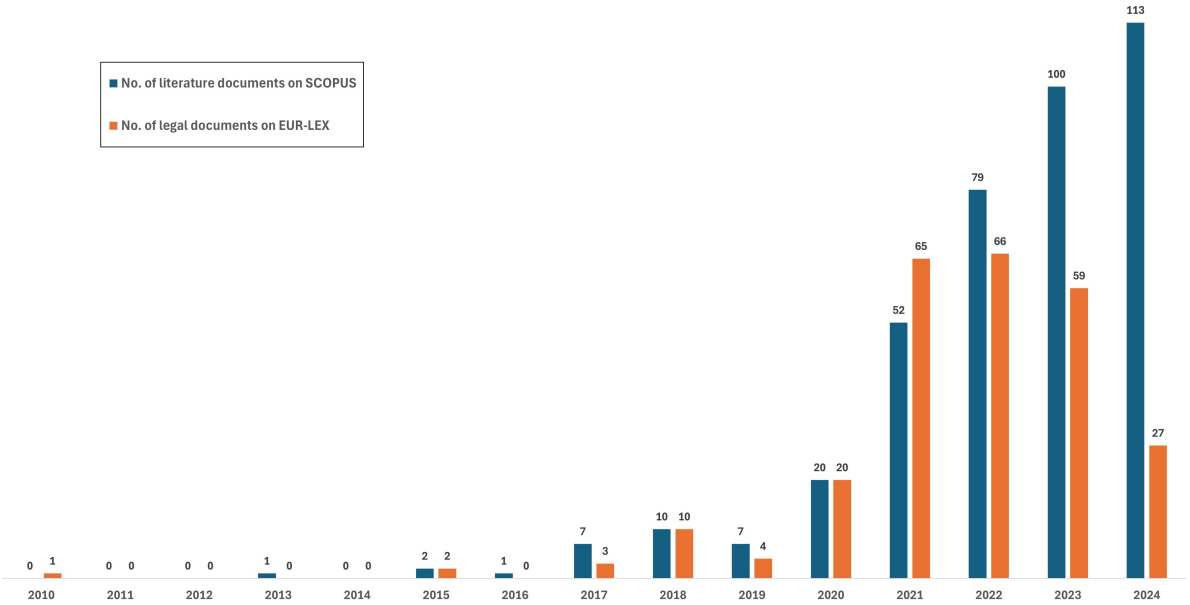

Figure 1: Number of documents on SCOPUS and Eur-Lex based on search term "digital sovereignty" (case-insensitive)

academic literature[Pedreira et al., 2021; Hellmeier and von Scherenberg, 2023; Meiring et al., 2023; Broeders et al., 2023a]. Consequently, scholars and policymakers are using these terms interchangeably across various topics and sectors, which is further diminishing the understanding of digital sovereignty.

Figure 1 presents the number of published documents in academic literature addressing "digital sovereignty"(case-insensitive) in the body of the text as compared to the number of published EU legal documents. To collect the published academic literature, we use one of the largest academic databases, Scopus, and to collect the legal documents, we use Eur-Lex, the official repository of EU legal documents. Academic literature on digital sovereignty started being published in 2013 and has been rapidly increasing since then, while the first address of digital sovereignty in EU legal texts was back in 2010. Both sectors saw a growth during the years from the year 2019, but unlike the academic literature, growth of such publications took a downward trend in EU policies after 2022. On closer inspection, we find that this is due to a decline in the overall publication of EU legal documents, indicating the impact of COVID-19 on the EU's legislative discourse.

2.2 Digital Sovereignty in EU policies

The discussion from Bangemann Report[3] and the communication on Growth, Competitiveness, and Employment[4] on the need for public-private partnership to encourage competitiveness and innovation laid the base for sovereignty in digital space in European political landscape. With the E-Commerce Directive[5], one of the EU's first regulatory initiatives that discussed the role of private sector actors over the Internet, the values behind the concept of digital sovereignty solidified. This legislative development matured within EU with the European Commission's policy communications, including the impact assessment document concerning the European Network and Information Security Agency (ENISA) efforts towards dealing with network and information security related issues[6], the opinion of the European

[3]Europe and the global information society: recommendations of the high-level group on information society to the Corfu European Council (No. S.2/94)

[4]Growth, competitiveness, employment: the challenges and the ways forward into the 21st century (NO. COM(93) 700)

[5]Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

[6]COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying document to the Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL concerning the European Network and Information Security Agency (ENISA)

Committee of the Regions on digital single market[7], cybersecurity strategy for the Digital Decade[8] and the Shaping Europe's Digital Future initiative[9], both of which assert that behavior in the digital environment should be governed by the same societal values and legislative accountability as in the physical world. Further, the European Data Governance Act[10] drew inspiration from the General Data Protection Regulation (GDPR), introducing restrictions on cross-border transfers of non-personal data to third countries.

The former German chancellor Angela Merkel, in her address at the 14th Internet Governance Forum (2019) clearly described her concerns over protection of Europe's digital assets, stating that "Digital sovereignty does not mean protectionism or the dictates of government agencies as to what information can be disseminated, but rather describes the ability to shape the digital transformation in a self-determined manner, whether as an individual, a single person, or as a society"[Merkel, 2019]. The following year in July, the European Commissioner Thierry Breton in a speech at Hannover Messe Digital Days, expressed that "in the face of growing tensions between the United States and China, Europe will not be a mere bystander, let alone a battleground. It is time to take our destiny into our own hands. This also means identifying and investing in the digital technologies that will underpin our sovereignty and our industrial future"[Breton, 2020].

More recently, various policies related to digitisation increasingly refer to the term *digital sovereignty* in their communications, including the Digital Decade Programme[11], the Chips Act[12] and Interoperable Europe.[13] The Digital Decade Programme provides a strategic framework to achieve digital goals by 2030. The Chips Act, established through regulation by the European Parliament and Council, aims to make Europe's semiconductor ecosystem more resilient. The Interoperable Europe Act supports public policies across Europe by emphasising the importance of public sector interoperability. New policy initiatives like the Digital Markets Act target unfair practices by big-tech platforms blocking competition and innovation[Bostoen, 2023]. The EU Cybersecurity Strategy supports new regulations on data, algorithms, markets, and network services within the Union[Bendiek and Kettemann, 2021] and the Network and Information Security Directive (NIS2) focuses on managing critical infrastructure.[14] All these policies are directed towards strengthening the idea of sovereignty in the European digital space, aiming to help companies protect their data, foster innovation and promote competitiveness aligning with Europe's economic, political, and societal objectives.

As current academic literature reveals a lack of contextual understanding of *digital sovereignty*, our work addresses this gap by systematically analyzing the legal and policy documents issued by the European Union, where *digital sovereignty* is discussed with greater frequency and detail[Bellanova et al., 2022]. Unlike previous studies, which predominantly rely on theoretical interpretations or normative claims, our approach leverages empirical data extracted from diverse EU legal documents. This allows us to provide a comprehensive and nuanced understanding of the concept, shedding light on both the motivations driving its adoption and the strategic goals it aims to achieve.

3 Methodology

To understand the motivation for and the intended goal of "Digital Sovereignty" as stated in EU legal documents, we empirically analyse the related text in these documents. We use the official repository of EU legal documents named "www.eur-lex.europa.eu" managed by the publication office of the European Union. Figure 2 illustrates the process of selecting and evaluating EU legal documents. First, we collect all the documents that satisfy our inclusion criteria and we filter out documents based on our exclusion

[7]Opinion of the European Committee of the Regions — digital single market

[8]JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The EU's Cybersecurity Strategy for the Digital Decade

[9]COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Shaping Europe's digital future

[10]REGULATION (EU) 2022/868 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)

[11]COMMISSION STAFF WORKING DOCUMENT Accompanying the document Proposal for a Decision of the European Parliament and of the Council establishing the 2030 Policy Programme "Path to the Digital Decade"

[12]REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act)

[13]COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act)

[14]https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

criteria, resulting in a total of 79 documents. Next, we select paragraphs that mention digital sovereignty in these documents and code various annotations within them that illustrate the motivation for and goal of digital sovereignty. Based on the number of codes obtained from the selected paragraphs for motivation and goals, we use various strategies for their analysis. To investigate the motivation, we manually identify themes by grouping similar motivation codes for a detailed analysis. In contrast, we explore the goals using data structures based on the Gioia method for the textual analysis of the selected paragraphs from the documents. Finally, we interpret our findings and discuss the key takeaways from our study.

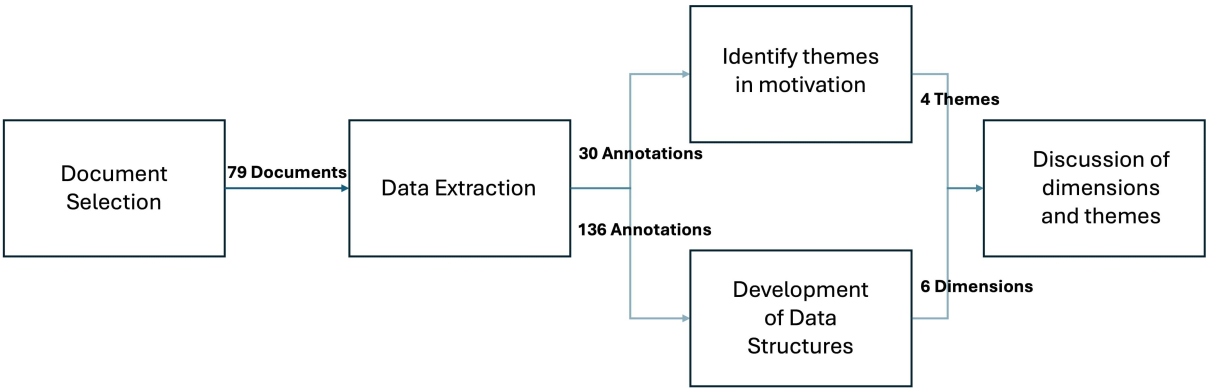

Figure 2: Methodology for selecting and evaluating EU legal documents.

3.1 Document Selection

Our study uses relevant political literature from the EU repository "www.eur-lex.europa.eu" containing more than 1.1 million records of legislative documents managed by the publications office of the European Union. To determine if a document should be included, we defined the following inclusion/exclusion criteria. Table 1 shows the count and reason for excluded documents during selection.

Inclusion Criteria:

Inclusion criteria helps us define the characteristics or properties of the documents we need to consider in our study. It is a method to filter documents from a large database, emphasising on the inclusion of as many relevant documents as possible to prevent critical emissions. We define three inclusion criteria for our document selection process.

IC1: The document includes the search term "digital sovereignty" (case-insensitive) either in its title or the body.

IC2: The document is in English.

IC3: The document is published by **May 2024**.

Exclusion Criteria: Exclusion criteria helps us define the characteristics or properties of the documents that we do not want to consider from our study. It is also a method to filter documents from a large database but it focuses on the eliminating of as many irrelevant documents as possible to ensure high precision of the study. We define four exclusion criteria for our document selection process.

EC1: The document is not properly referenced on the repository. A properly referenced document has its reference number(CELEX No.), type(Form), and categorization(Directory Code) present in the repository.

EC2: The document does not present the latest communication related to the legislative/policy communication by the Union.

EC3: The document is not publicly available for download. Some documents have been moved or are only available for reading online.

EC4: The document is either too specific, too abstract or provides insufficient information that can contribute to our study. Some examples of such documents are abstracts, case laws, judgments, verbatim reports, notices, summaries, specific implementations, and country-specific communication, among others.

The initial search returned 248 documents of various sizes from the platform. The number of pages in a single document ranged from 3 pages, such as in the Commission Implementing Decision of 7 December 2022 on the financing of the European Innovation Council, to around 2300 pages, such as in the European

Category	Details	Count
Included Documents	IC1, IC2, IC3	248
Excluded Documents	EC1	120
	EC2	6
	EC3	9
	EC4	34
Selected Documents		79

Table 1: Summary of Document Selection Process

Union's general budget for the financial year 2021. Based on the above inclusion and exclusion criteria, we select 79 documents.

3.2 Data Extraction

For the next steps of our study, we extract relevant text from the 79 different forms of documents that we screened. To explore the EU's motivation behind pushing for *digital sovereignty* and its goals as described in the EU legal documents, we select the paragraphs of the selected documents where *digital sovereignty* is addressed and annotate texts that mention the *motivation* for and *goals* of digital sovereignty. We ensure that the selection is significantly large to preserve the context. In the selected documents, we manually annotated 30 *motivation* and 136 *goals* using the Atlas.ti tool.

3.3 Identify Themes in Motivation

We identify 30 annotations in the selected paragraphs from the 79 documents that relate to the motivation for enforcing digital sovereignty in EU. We manually identify recurring themes in these annotations. Table 2 shows a few examples of annotations and their corresponding concepts. To prevent bias in the coding process, we follow a multi-author validation strategy, once the first author had coded all annotations, two other authors independently reviewed the codes. The three authors then collectively discussed conflicts in coding to resolve discrepancies.

3.4 Development of Data Structures for Goals

We use the Gioia approach to help us examine the goals of digital sovereignty systematically. The Gioia method is known for its transparency and replicability, which is formulated on reasoning-based linking of similar concepts into higher-level conclusions, providing a structured framework for qualitative research of complex topics. This structural method for information retrieval helps us systematically and rigorously establish an empirical model for understanding digital sovereignty grounded in empirical data, known as a data structure. It ensures transparency and traceability throughout our research process, illustrating the grounding of the high-level theoretical interpretation and visualising the logical flow of the analysis.

We use a data structure to explore the goals of digital sovereignty from 136 annotations layering the codes into more abstract themes and dimensions. Table 3 shows examples of annotations that mention goals and their corresponding 1st-order concepts. We draw 40 codes suitable to be consolidated into 12 abstract and disjoint 2nd order themes. Again, to avoid bias we follow a multi-author validation strategy as explained previously. Next, we create a data structure based on the interpretation of the empirical data to categorise six dimensions defining the goals of digital sovereignty in EU legal documents.

3.5 Discussion of Dimensions and Themes

We present the themes representing the motivation for and goals of digital sovereignty, interpreting the themes with proofs from EU legal documents to gain contextual insights from the empirical data. Using the annotations related to each theme, we discuss their relevance and relation to building the understanding of digital sovereignty from the lens of EU legal documents. At last, we combine our thematic interpretation of the motivation behind the EU's push for digital sovereignty and the dimensions of digital sovereignty goals with the help of their theoretical relationship at different levels to answer our research question, guiding future policymakers and researchers.

Document No.	Example Motivation Annotation	Concept codes
52022IE2134	"Despite significant progress to enhance the EU's digital sovereignty, there is still heavy reliance on non-EU-based tech companies. This is limiting the EU's leadership and strategic autonomy in the digital world, and in turn limiting the EU's economic growth potential."	Reliance on non-EU based companies
52022SC0721	"Both the problem and problem drivers show that the current policy approach, based solely on voluntary measures at Member States level and no coordination at EU level, is not fit for purpose. They increase costs and reduce efficiencies at all levels of public administrations in the European Union, add administrative burdens on citizens, businesses and administrations themselves, delay the implementation of European policies by the Member States and the accomplishment of the Digital Single Market, limit the potential to innovate and hinder the EU's digital sovereignty."	Lack of coordination among Member States
52022IE2134	"The EESC argues that the existing imbalances in digital sovereignty are partly due to national barriers that continue to impede the achievement of a genuine Single Market. As things stand, the Single Market is essentially a compound of multiple smaller national markets, without the scale needed for any single EU-based company to compete with the digital giants of this world. In addition, there are different levels of digital development, infrastructures and capacities across the EU."	National barriers to single market
52022IE1011	"Large amounts of data are now available to public authorities and a handful of big tech giants such as Google, Facebook (Meta), TikTok or Amazon. Unfortunately, only a limited number of stakeholders benefit today from it and the EESC is worried that the data produced in the EU is stored, processed and produces value outside Europe. The Committee considers that EU digital sovereignty will be hard to achieve without its own EU digital tech giants, without storing European data on EU soil and without protection of these data from any extra-territorial access."	Limited control over EU's data
32024H0779	"Our economies and societies are increasingly reliant on the functioning of the internet and of international connectivity to achieve the competitive digitalisation of the Union and its economy. In this context, submarine cable infrastructure is a significant element in the broader internet ecosystem in achieving European digital sovereignty, given that the overwhelming majority of international data traffic is carried through submarine cables."	Dependencies on critical infrastructures

Table 2: Examples annotations for Digital Sovereignty Motivation and Respective concept codes

Document No.	Example Goal Annotation	1st Order Concept Code
52021IR5656	"The EU's digital sovereignty will depend on capacity to store, extract and process data, while satisfying the requirements of trust, security and fundamental rights."	Strategise Management of EU Data
52021SC0247	"Address key strategic digital technologies and would be part of the EU's attempt to reinforce its digital sovereignty, carefully monitoring, assessing and addressing any strategic dependencies weaknesses and vulnerabilities which put at risk the attainment of its digital ambitions as well as its capacity to shape a digital transformation that reflects its values."	Identify Strategic Technological Dependencies
32022D2481	"The Union's path to the digital transformation of the economy and society should encompass digital sovereignty in an open manner, respect for fundamental rights, the rule of law and democracy, inclusion, accessibility, equality, sustainability, resilience, security, improving quality of life, the availability of services and respect for citizens' rights and aspirations."	Digitisation of Europe based on the EU values
52021AE4854	"Digital sovereignty needs to be based on competitiveness that relies on solid cooperation between Member States, accompanied by the intrinsic involvement of civil society stakeholders, including businesses, workers, consumers, academia and other relevant stakeholders."	Cooperation among the European Member States
52022IE5106	"The EU must build resilience to cyberattacks and create effective cyber deterrence. Critical infrastructure must be protected against cyberattacks of all kind, including by EU defence systems. The Committee considers it to be in the EU's strategic interest to ensure that the Union retains and develops the essential capacities to secure its digital economy, society and democracy, to achieve full digital sovereignty as the only way to protect critical technologies and to provide effective key cybersecurity services."	Enhance Cybersecurity and Defence Capabilities

Table 3: Examples annotations for Digital Sovereignty Goals and 1st order concepts

4 Findings and Discussion

In line with the study's objectives, we divide this section into three parts. First, we investigate the corpus of documents we select in our study to understand the sectors/directories they relate to. This provides us with information on the relevance of digital sovereignty and its intensity in various fields. Second, we analyse EU's motivation for digital sovereignty, helping us apprehend the current challenges and underlying problems faced by the EU. Finally, we explore the goals of digital sovereignty as described in the EU policies/programmes to reveal the Union's intentions and strategies for future digital policies.

4.1 Exploration of selected legal documents

In this section, we investigate the broad characteristics of the selected legal documents. We observe that the documents we screened for our analysis are distributed over various directories and categories. The directories is used to organise the documents based on their relevance to a topic or sector while the categories define type of the legal documents, helpful in estimating its legal boundaries and current implementation requirements.

Figure 3 provides information on the publication of documents in various areas of political interest for the Union. We observe that the first reference to digital sovereignty in EU policy communication in

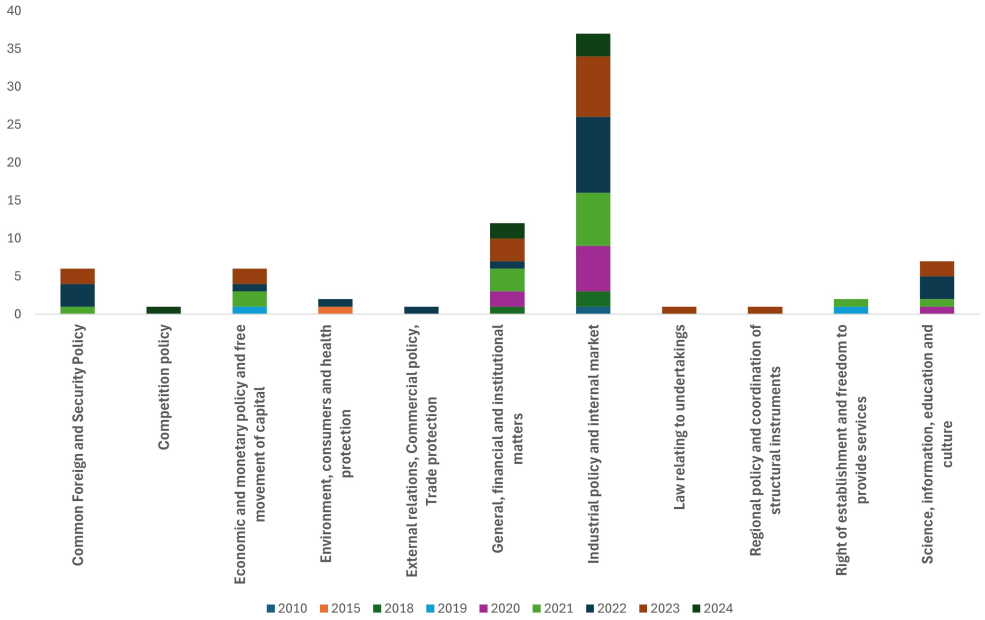

Figure 3: Directory-wise yearly representation of the selected EU policy documents

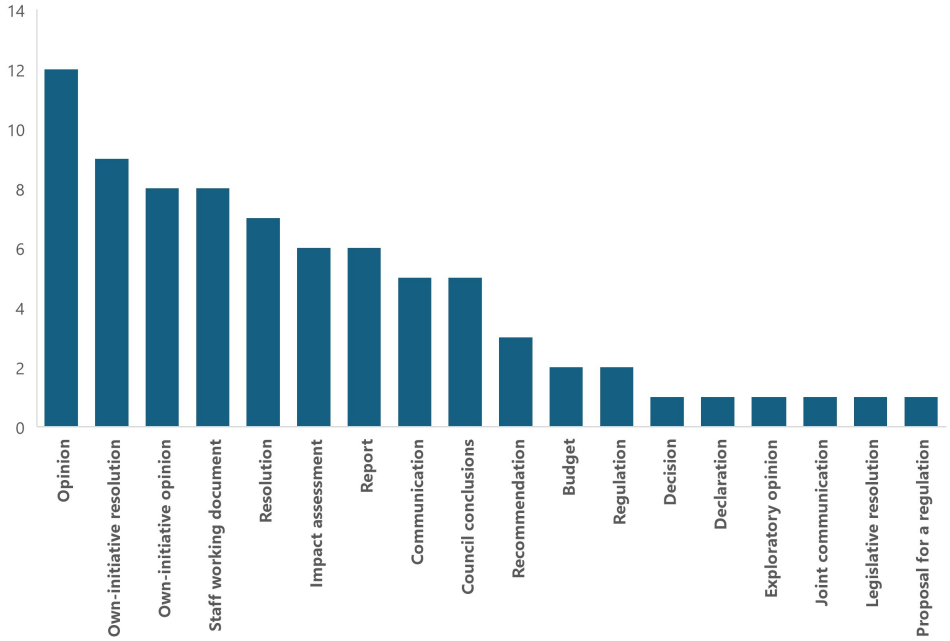

Figure 4: Representation of diversity in the dataset: Count of different forms of EU legal documents

2010 was published in the Directory of Industrial Policy and Internal Market. We also find that 48.2% of policy documents in our corpus belonged to the Industrial Policy and Internal Market directory, while another 15.2% of documents belonged to the directory of general, financial and institutional matters. The significant gap between the size of the largest and second-largest groups of documents indicates that digital sovereignty is substantially addressed within the context of industrial policy and the internal market of Europe, followed by financial and institutional matters. This strengthens our notion that with digital sovereignty, the EU focuses on the industrial, institutional, and internal market challenges emerging from the lack of cooperation between member states or the dependence on foreign digital networks. It also aligns with the Union's digital single market strategy, ensuring that Europe's economy, industry, and society make full use of the opportunities provided by the digital era.

Figure 4 illustrates the representation of various types of legal documents present in our selected corpus. We observe that the highest number of documents are opinions by European institutions, indicating

the nascent stage at which digital sovereignty is being discussed in European policies. Although there are only a few legislative documents specifically addressing digital sovereignty, we observe a significant presence of this topic in preparatory, assessment, and own-initiative documents. This trend indicates a proactive effort by European institutions to ensure that the EU's policies align with the principles of digital sovereignty. Nonetheless, we see a wide variety of documents contributing to the ongoing discussions on digital sovereignty.

4.2 Motivation for Digital Sovereignty

We find that the motivation behind digital sovereignty can be classified in four themes: **Increasing foreign digital dependencies and dominance**, **Lack of common digital governance and regulation**, **Insufficient security and increasing threats**, and **Increasing social and economic impact of technology**.

Increasing foreign digital dependencies

Europe is increasingly concerned about its growing dependency on foreign digital platforms and the dominance of non-EU tech companies. This dependency undermines the resilience of its digital infrastructure and raises critical questions about the security of European citizens' digital identity and data. These concerns are shared in the European Economic and Social Committee (EESC)'s opinion on digital identity, data sovereignty, and the path to a just digital transition for citizens in the information society:

> "Large amounts of data are now available to public authorities and a handful of big tech giants such as Google, Facebook (Meta), TikTok or Amazon. Unfortunately, only a limited number of stakeholders benefit today from it and the EESC is worried that the data produced in the EU is stored, processed and produces value outside Europe."[15]

The lack of compliance with European regulations like the General Data Protection Regulation (GDPR) by these dominant tech companies highlights a misalignment of values and priorities. This leads to significant risks, including the unlawful processing and misuse of European data. Reflecting on this reliance, the EESC in its opinion on Digital Sovereignty notes:

> "For far too long, concern has been expressed about the heavy reliance of the EU on a small number of large tech companies operating outside the EU."[16]

While these platforms contribute significantly to economic growth, they also restrict the EU's control over its digital data, undermining trust in online information. The EESC notes this issue in its opinion on digital sovereignty:

> "In an online environment still dominated by non-EU tech companies, the question arises as to the degree of control EU citizens, businesses and governments may have over their digital data. This may not appear to be a priority in the current crisis, but the need to address the digital sovereignty imbalance cannot downplayed."[16]

The problem is worsened by the over-reliance on foreign platforms in key economic sectors. This dependence hampers the EU's ability to assert its sovereignty in crucial areas like copyright, data protection, and taxation. EESC states:

> "Worryingly, entire sectors of the EU economy remain heavily dependent on large, non-EU based online platforms. This deprives Member States of their digital sovereignty in key areas such as copyright, data protection, and taxation. This concern has also been extended to other areas such as e-commerce and online disinformation."[16]

Despite advancements in digital sovereignty, the EESC emphasizes that the EU remains significantly dependent on non-EU tech companies, which stifles its leadership and limits its economic potential:

[15] Opinion of the European Economic and Social Committee on digital identity, data sovereignty and the path to a just digital transition for citizens living in the information society (own-initiative opinion)

[16] Opinion of the European Economic and Social Committee on Digital Sovereignty: a crucial pillar for EU's digitalisation and growth (own-initiative opinion)

"Despite significant progress to enhance the EU's digital sovereignty, there is still heavy reliance on non-EU-based tech companies. This is limiting the EU's leadership and strategic autonomy in the digital world, and in turn limiting the EU's economic growth potential." [16]

Key Takeaway: Such extensive dependency restricts Europe's ability to independently navigate global cyberspace, protect its economic interests, and ensure democratic resilience. Non-transparent and unsupervised features of foreign platforms pose further risks, as their operations often lack alignment with values that the EU considers fundamental. Data collected by these platforms primarily benefits non-EU companies, placing European digital strategies and democratic processes at risk. This dominance limits Europe's digital growth and highlights the urgent need for achieving digital sovereignty, enabling the EU to build a secure, fair, and transparent digital ecosystem aligned with its core values.

Lack of common digital governance

Despite various digital governance policies and regulations enacted by European member states, their efforts often fail to produce significant value. Fragmented strategies, delays in implementing EU-wide policies, and a lack of tools for cooperation among member states hinder the path toward global digital leadership. These challenges also slow progress toward achieving a Digital Single Market, which seeks to unify the digital needs and aspirations of all member states. The working document on establishing high public sector interoperability across the Union highlights these shortcomings:

"Both the problem and problem drivers show that the current policy approach, based solely on voluntary measures at Member States level and no coordination at EU level, is not fit for purpose. They increase costs and reduce efficiencies at all levels of public administrations in the European Union, add administrative burdens on citizens, businesses and administrations themselves, delay the implementation of European policies by the Member States and the accomplishment of the Digital Single Market, limit the potential to innovate and hinder the EU's digital sovereignty." [13]

The absence of a unified governance and legislative framework in the digital domain also stifles innovation and constrains the growth of domestic businesses. Member states' conflicting regulatory approaches restrict operational scope, making it difficult for small and medium-sized enterprises (SMEs) to navigate administrative requirements and expand across Europe. This often drives these businesses to partner with non-European companies or relocate entirely. As highlighted by the European Parliament in its resolutions on Artificial Intelligence:

"Unclear, excessive or fragmented regulation will hampers the emergence of innovative high-tech unicorns, start-ups and SMEs or drive them to develop their products and services outside of Europe." [34]

The lack of coherence in legislative frameworks also limits the adoption and integration of emerging technologies across the Union. This disjointed approach undermines Europe's ability to support innovative solutions that require cross-border collaboration. The European Parliament further emphasizes:

"This cannot be sufficiently achieved by the Member States due to the rapid technological change, the cross-border development as well as the usage of AI-systems and eventually, the conflicting legislative approaches across the Union." [17]

Nation states strive to maintain their global competitiveness by fostering regionally developed innovations that leverage European resources and talent. However, without a common governance framework, Europe's digital ecosystem remains fragmented, limiting its potential as a unified digital market. Such a framework would bolster the EU's global position and strengthen its digital sovereignty by supporting start-ups and SMEs to reduce dependency on foreign big-tech companies. The EESC underscores this necessity in its opinion on digital sovereignty:

"The existing imbalances in digital sovereignty are partly due to national barriers that continue to impede the achievement of a genuine Single Market." [16]

[17] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence (2020/2014(INL))

Key Takeaway: These national barriers arise from member states prioritizing their individual interests in cyberspace over a unified European approach. While such individual strategies may yield short-term benefits, they ultimately weaken the EU's ability to develop and procure critical technologies and resources. The long-term economic implications of this fragmentation are profound, affecting all member states. Addressing these challenges through unified governance and coordinated policies is essential for creating a cohesive digital ecosystem and achieving the EU's goal of digital sovereignty.

Insufficient security amid rising threats

In the current state of international affairs where there are a lot of conflicts among countries, the security of critical infrastructures is crucial. These critical infrastructures range from telecommunication cables to raw materials used for the production of digital products. One such case is the impact of ongoing conflict between Russia and Ukraine on Europe's resilience in semiconductor technologies among others. In the opinion establishing the Joint Undertakings under Horizon Europe, EESC argues that,

> "Russia's war against Ukraine is likely to have many side effects in the medium to long term for the semiconductor industry, a top priority for EU digital sovereignty. The production of neon, palladium and C4 F6, three materials that are crucial and irreplaceable for microchips, will be impacted by the situation."[18]

Beyond resource vulnerabilities, critical digital infrastructures such as submarine cables represent single points of failure in the global ecosystem. Recent events have underscored the risks to these infrastructures, raising concerns about their security amid transnational conflicts. The European Commission emphasizes the importance of resilient submarine cable systems:

> "In the current context of heightened risk and antagonistic man-made security threats, given the interconnected and transnational nature of these infrastructures, governments in all world regions are paying particular attention to their potential reliance on critical cables, as systemic and widespread disruptions of submarine cable communications could lead to particularly serious consequences, in case of coordinated attacks."[19]

To preserve the digital sovereignty of Europe, the resilience of critical infrastructure should be secured, and strategies need to be devised to ensure sufficient safeguards are in place to mitigate any risk and defend against any attack coming toward Europe. Due to high dependencies on foreign technologies and platforms complementing the national barriers hindering the common strategy for digital governance, it is becoming difficult for EU to tackle upcoming threats for its digital economic growth. The European Parliament, in its 2022 annual report on the common foreign and security policy, highlights the dangers posed by new digital technologies:

> "the specific threat that the new digital technologies pose for human rights defenders and others because they can be used for controlling, restricting and undermining their activities."[20]

Similarly, foreign interference on social media has emerged as a significant threat to Europe's democratic fabric. The EU's general budget for 2022 underscores the critical need to combat such interference:

> "foreign interference on social media has become a real threat to democracy and the cohesion of Europe. The narrative on the Union and Europe must be driven by Europeans and not handed over to foreign sources intended on weakening European cohesion."[21]

Key Takeaway: These multifaceted threats not only undermine Europe's societal and economic stability but also exacerbate inequalities in the global digital marketplace. A robust and unified digital strategy is essential to address these vulnerabilities. Such a strategy must include governance models

[18] Opinion of the European Economic and Social Committee on 'Proposal for a Council Regulation amending Regulation (EU) 2021/2085 establishing the Joint Undertakings under Horizon Europe, as regards the Chips Joint Undertaking' (COM(2022) 47 final — 2022/0033 (NLE))

[19] Commission Recommendation (EU) 2024/779 of 26 February 2024 on Secure and Resilient Submarine Cable Infrastructures

[20] European Parliament resolution of 18 January 2023 on the implementation of the common foreign and security policy — annual report 2022 (2022/2048(INI))

[21] Definitive adoption (EU, Euratom) 2022/182 of the European Union's general budget for the financial year 2022

that bolster Europe's security and defense capabilities, enabling sustainable development and protecting the Union from external cyber threats.

Growing social and economic impact of technology

The COVID-19 pandemic significantly impacted global business practices, accelerating the shift to digital markets. Although these digital technologies and platforms helped businesses and organisation to sustain their operations while broadening the options for consumers, they also made the society more vulnerable to unethical and unfair practices. The European Economic and Social Committee (EESC), in its proposal for the Digital Services Act, highlights this issue:

> "With the COVID-19 crisis, the sale of unsafe products, fake reviews, unfair commercial practices and other consumer law violations, piracy and counterfeiting on digital platforms rose to unacceptable levels." [22]

These practices erode consumer trust, compromise operational resilience, and threaten the financial stability of the Union. While digital platforms have expanded global markets, they have also enabled unlawful firms to exploit European consumers, often without immediate repercussions. This concern is echoed in the European Commission's 40th annual report on trade defense, which warns:

> "Without measures to address the unfair trade practices of the Chinese exporters, the future of the EU industry would be jeopardised as it would face further financial deterioration in terms of profitability and investments." [23]

To mitigate such challenges, the EU must enforce measures and establish common regulations for both online and offline markets. Additionally, strategies to reduce societal reliance on potentially exploitative platforms, or the development of robust safeguards, are essential to ensure the safety of EU citizens in the digital age. The increasing dependence on digital technologies has also amplified exposure to cyber fraud, cyberattacks, and misinformation. Reflecting on the lessons from the pandemic, the EESC points out:

> "Lessons learned during the current pandemic, which has shown that the increasing dependence of society and the economy on digital solutions leaves them vulnerable and exposed to growing and rapidly changing cyber threats, especially with regard to groups at risk of social exclusion such as people with disabilities." [24]

> "Our economies and societies are increasingly reliant on the functioning of the internet and of international connectivity to achieve the competitive digitalisation of the Union and its economy." [19]

While digital technologies foster economic growth and societal transformation, they also expose vulnerabilities. The lack of equitable access and robust infrastructure risks deepening the digital divide, limiting opportunities for marginalized communities, and exacerbating inequalities. The European Parliament and the Council, in their regulation on gigabit networks, stress the importance of addressing this issue:

> "Limited access and insufficient network expansion can deepen social inequalities, thus creating a new digital divide between people who are able to benefit fully from an efficient and secure digital connectivity, allowing them to access a wide range of services, and people who are unable to do so." [25]

[22] Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC' (COM(2020) 825 final — 2020/0361 (COD))

[23] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL 40th Annual Report from the Commission to the European Parliament and the Council on the EU's Anti-Dumping, Anti-Subsidy and Safeguard activities and the Use of Trade Defence Instruments by Third Countries targeting the EU in 2021

[24] Opinion of the European Economic and Social Committee on 'Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 and Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities' (COM(2020) 823 final — 2020/0359 (COD) — COM(2020) 829 final — 2020/0365 (COD))

[25] Regulation (EU) 2024/1309 of the European Parliament and of the Council of 29 April 2024 on measures to reduce the cost of deploying gigabit electronic communications networks, amending Regulation (EU) 2015/2120 and repealing Directive 2014/61/EU (Gigabit Infrastructure Act) (Text with EEA relevance)

Key Takeaway: The dual impact of digital technologies—enabling innovation and exposing vulnerabilities—necessitates careful administration. Proper governance of these technologies can enhance their benefits while minimizing risks. Addressing unlawful practices, reducing the digital divide, and protecting vulnerable groups will help the EU define and achieve its goals for digital sovereignty, ensuring a fair, secure, and inclusive digital ecosystem.

4.3 Goals of Digital Sovereignty

With the help of the data structure based on the gioia methodology, we explore the goals of digital sovereignty in the EU policy documents. Our exploration provides us with six dimensions, namely **strategic capabilities**, **EU-based production and innovation**, **complaint and open cyberspace**, **autonomous decision making**, **interoperable and standard market**, and **Value-based digital transformation** that represent its core objectives. The goals of digital sovereignty clearly define the context in which the European Union addresses the notion of digital sovereignty and its future potential.

Figure 5 shows the data structure representing the six dimensions that constitute the core focus of digital sovereignty in the EU policy documents. It consists of data extracted from the documents addressing digital sovereignty in their body of text. We consolidated similar 1st order concepts from our coding process to develop twelve abstract themes that helped us explore the answer to our research question. To demonstrate our empirical observations, which could be used to define the context in which digital sovereignty is used in EU policy documents, we highlight key informant quotes that make up the final dimensions of the goals of digital sovereignty in our study.

4.3.1 Data Control

We exist in a data-driven economy where most of the data generated by individuals is stored and analyzed by businesses to improve decision-making, optimize operations, and enhance consumer experiences for business growth. One of the dimensions of digital sovereignty aims to ensure that data generated within the European borders is used in accordance with its laws and with respect to its values, such as the General Data Protection Regulation(GDPR).

Framework for the management of European data

Currently, there is a need to set global standards for trustworthy data technologies in all sectors, with digital technologies at their core. Such standards enable the secure exchange of data across various organisations, enhancing business operations and promoting innovation. Additionally, a common framework for European data will help to standardise the data operations across public and private institutions of Europe, impacting global digital markets. In its opinion on strengthening EU's clearing systems, EESC

> "Promotes data-driven finance and considerably improves access by companies, businesses and financial institutions to data and entities' information, as well as making the economy fit for the digital future, strengthening digital sovereignty, increasing the speed of information flow and setting common standards, with a focus on data, technology and infrastructure". [26]

Standardisation of data helps in enhancing the flow of information while enhancing the data access and data management ability of European businesses and service providers, reducing reliance on third-party platforms. To create a common framework based on standardised data generated within Europe, strategies for its management and exchange should be devised to reduce reliance on foreign companies, build interoperability across EU-based institutions and support the development of an inclusive digital economy. In an opinion on new prospects and challenges for European products and services, EESC advocates that

> "Data access and data management ability is the next area of policy intervention that refers to the purpose of supporting European producers and service providers in responding to the

[26] Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council, the European Central Bank and the European Economic and Social Committee – A path towards a stronger EU clearing system'(COM(2022) 696 final) and on the 'Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 648/2012, (EU) No 575/2013 and (EU) 2017/1131 as regards measures to mitigate excessive exposures to third-country central counterparties and improve the efficiency of Union clearing markets'

Figure 5: Data Structure: a graphic representation of the context digital sovereignty themes and dimensions in EU policy documents

contemporary evolution of globalised markets and utilising their comparative advantage in highly specialised goods and services. This is especially essential for SMEs. Nevertheless, freeing data access goes hand in hand with an increasing risk of data abuse. Ensuring both digital sovereignty and the privacy of natural and legal persons may be a technically and legally difficult task, yet at the same time essential."[27]

With a common framework for storing, extracting and processing data, Europe will gain a competitive advantage in global digital markets, provide its citizens with exclusive products & services, and substantially reduce the risk of data abuse. Nonetheless, the management of data requires extreme care with regard to ensuring the ethical use and protection of data, which is categorised as personal or critical as defined by GDPR. In the strategic foresight report, the European Commission argues:

"the EU's digital sovereignty will depend on capacity to store, extract and process data, while satisfying the requirements of trust, security and fundamental rights."[28]

Key Takeaway: To satisfy the requirements of fundamental rights, EU emphasises on the identification and protection of personal data should be a priority in the data management plan of organisations.Although managing data in business operations can be challenging, strategies such as anonymisation, pseudonymisation, data minimisation, and encryption can aid in effective data management while ensuring compliance and maximising benefits. Developing a common framework with an ethical data culture, building on trust with stakeholders, and ensuring the security of sensitive information, is a prerequisite for Europe's sovereignty over cyberspace..

4.3.2 Democratic digital transformation

As Europe accelerates the digital transformation of its economy and society, it aims to ensure that the digital ecosystem reflects its democratic values and human rights. These democratic value consists of fairness, freedom, equality, respect for the rule of law, and social justice, together formulating the foundation of a just society and fair economy. Digital sovereignty can be preserved when all stakeholders involved in the digital transformation respect the democratic principles that Europe abides by.

Digitisation based on EU values and fundamental rights

Economic goals of Europe focus on key values that aim to provide a fair and high-quality life for all its citizens. It now aims to extend these principles to the digital space, which lacks structure, transparency, and control. The Union aims to develop a digital ecosystem that is open, accessible and based on the democratic principles that Union stands by. It aims to ensure that digitisation in Europe contributes to a resource-efficient economy and a fair society, making it more inclusive. In the decision on the Digital Decade Policy Programme 2030, the European Parliament and the Council stresses on

"Promoting a human-centred, fundamental-rights-based, inclusive, transparent and open digital environment where secure and interoperable digital technologies and services observe and enhance Union principles, rights and values and are accessible to all, everywhere in the Union." [29]

"The Union's path to the digital transformation of the economy and society should encompass digital sovereignty in an open manner, respect for fundamental rights, the rule of law and democracy, inclusion, accessibility, equality, sustainability, resilience, security, improving quality of life, the availability of services and respect for citizens' rights and aspirations. It should contribute to a dynamic, resource-efficient, and fair economy and society in the Union."[29]

Digital transformation is a very abstract dimension that overlaps with many other dimensions, but for Europe, it has important aspects of preserving European values as a guiding principle of its digital and innovation policies. The focus of digital sovereignty is to push Europe towards value-based digital

[27]Opinion of the European Economic and Social Committee on 'Use-value' is back: new prospects and challenges for European products and services (own-initiative opinion)

[28]COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL 2021 Strategic Foresight Report The EU's capacity and freedom to act

[29]Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (Text with EEA relevance)

transformation, which empowers its citizens and societies. In its resolution of 17 January 2024 on policy implications of the development of virtual worlds, the European Parliament finds that

> "Digital sovereignty is a means of promoting the notion of European leadership and strategic autonomy and is key to guaranteeing the EU's ability to shape and enforce legislation in the digital environment, ensuring ethical, sustainable and human-centric virtual worlds and safeguarding the fundamental rights and values of the EU." [30]

Key Takeaway: Digital sovereignty aims to ensure that Europe's digital transformation is just and reflects democratic principles. The values on which the EU is founded, namely, Human dignity, Freedom, Democracy, Equality, Rule of law, and Human rights must also be protected in the digital space to facilitate the digitisation of European society and ensure inclusive and sustainable economic growth.

Boosting digitalisation across Europe

With the increase in technological innovation and the development of new digital solutions, global cyberspace is evolving rapidly. Events like the COVID-19 pandemic and advancements in AI technologies have deepened the economic dependence on technology across all sectors. In its opinion on the Path to Digital Decade Programme, EESC also establishes that

> "COVID-19 has revealed the critical importance of technology for economic and health resilience, making the EU's digital transformation and sovereignty a matter of existential importance. The European Economic and Social Committee (EESC) therefore urges the EU to develop its digital sovereignty, which over the coming years is expected to be a crucial pillar of Europe's path to economic, social and environmental development." [31]

To ensure the continuous growth of its economy and society, Europe must facilitate the digital transformation of its industries and institutions to drive innovation, enhance competitiveness, and ensure sustainability in a world that is more connected than ever. Accelerating the digital transition of the economy and society is a priority for all nations, as it ensures they maintain their competitive edge in innovation and growth on a global scale. For example, in Germany's 2022 digital decade strategy, the European Commission stresses that

> "The country's technological and digital sovereignty is the guiding principle for its digital and innovation policy. Before this, Germany had already introduced several strategies, initiatives and activities to support the digital transformation of companies and the deployment and uptake of advanced technologies. Several measures are specifically tailored to SMEs."[32]

It is essential to support emerging digital businesses based in the EU that promote innovation, facilitate digital transition, and help reduce the digital gap among various economies within the Union. Digital solutions help increase productivity and boost innovation in the economy. When drafting the general budget for the financial year 2022, the European Council stresses on

> "The need to bridge the digital divide and strengthen the Union's resilience and digital sovereignty; believes that the Digital Europe Programme is a vital tool in increasing rates of digitalisation in the Union, thereby leading to significant productivity gains, and in helping to bolster investments in cybersecurity and artificial intelligence" [33]

Key Takeaway: With digital sovereignty, the Union seeks to boost digitisation of the society based on democratic values and principles. A democratic digital transformation of Europe focuses on bridging the digital divide among its various economies, as this obstructs a unified digital governance framework and undermines its strategic digital autonomy.

[30] Policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues – European Parliament resolution of 17 January 2024 on policy implications of the development of virtual worlds – civil, company, commercial and intellectual property law issues (2023/2062(INI))

[31] Opinion of the European Economic and Social Committee on Proposal for a decision of the European Parliament and of the Council establishing the 2030 Policy Programme 'Path to the Digital Decade' (COM(2021) 574 final — 2021/0293 (COD))

[32] COMMISSION STAFF WORKING DOCUMENT Digital Decade Country Reports Accompanying the document Communication from the Commission to the European Parlaiment, the Council, the European Economic and Social Committee and the Committee of the Regions Report on the state of the Digital Decade 2023

[33] European Parliament resolution of 21 October 2021 on the Council position on the draft general budget of the European Union for the financial year 2022 (11352/2021 — C9-0353/2021 — 2021/0227(BUD))

4.3.3 Open Strategic Autonomy

Open strategic autonomy is the ability to safeguard one's interests while ensuring fair and equitable participation in global digital markets. In the current cyberspace, heavily influenced by the tech-giants from the U.S. and China, the Union aims to reduce its dependence on non-European technology providers, ensuring the competitiveness of its industries while securing the critical digital infrastructures and technologies.and services remain secure and aligned with EU values. It also includes developing its own domestic capabilities and protecting European digital assets from geopolitical risks and exploitation.

Strategies for global digital governance

The Union's strategic technological dependencies on foreign entities range from software like operating systems and services like Google and Facebook to hardware like microchips and submarine cables. Europe's digital future heavily relies on identifying and addressing such dependencies with long-term action plans. The European Parliament, in its resolution on shaping the digital future of Europe

> "Highlights that investing in sciences, research and development in the areas of digital and AI, fostering better access to venture capital, developing a strong cybersecurity of critical infrastructures and electronic communication networks and access to unbiased high-quality data are the cornerstones of ensuring the digital sovereignty of the Union; calls on the Commission to study the different ways in which the Union is at risk of becoming dependent on external players; notes that unclear, excessive or fragmented regulation will hampers the emergence of innovative high-tech unicorns, start-ups and SMEs or drive them to develop their products and services outside of Europe;" [34]

The European Union is not only dependent on external players but also on its Member States for implementation of regulations and programmes. This hinders innovation as well as Europe's capacity to produce domestic technologies and solutions. The ability to make autonomous decisions and act independently constitutes the core of digital sovereignty. According to the European Commission's report on the state of the Digital Decade 2023,

> "Digital sovereignty refers to our ability to act independently in the digital world, and therefore it constitutes a crucial means to safeguard our values".[35]

The dimension of autonomous decision-making is highly relevant for the EU to ensure competitiveness in digital markets and pave its way toward global leadership in cyberspace, which can be facilitated by the creation of a digital single market within Europe. A single market simplifies the implementation of decisions through a unified digital agenda. The Annual Report on Research and Technological Development Activities of the European Union and Monitoring of Horizon 2020 states that

> "The EU must build a truly digital single market, secure digital sovereignty, develop and deploy strategic digital technologies, capacities and infrastructure, in order to reinforce its ability to define its own rules and make autonomous technological choices accordingly."[36]

With a single digital market and autonomous decision-making capabilities, Europe will be able to create a unified digital governance framework with effective measures to secure its economic and strategic interests. Given the current landscape, where numerous regulations and policies already aim to secure Europe's strategic autonomy and uphold its digital sovereignty, it is crucial to evaluate their implementation and effects regularly. This is essential for shaping future policies and formulating effective strategies to combat foreign interference. In the decision to establish the Digital Decade Policy Programme 2030, the European Parliament and the Council discuss investigating the effect of the programme, suggesting that

> "The Commission should address in its Report on the Digital Decade how effectively the general objectives of this Decision have been implemented into policies, measures or actions,

[34] European Parliament resolution of 20 May 2021 on shaping the digital future of Europe: removing barriers to the functioning of the digital single market and improving the use of AI for European consumers (2020/2216(INI))

[35] COMMISSION STAFF WORKING DOCUMENT Implementation of the Digital Decade objectives and the Digital Rights and Principles Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Report on the state of the Digital Decade 2023

[36] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Annual Report on Research and Technological Development Activities of the European Union and Monitoring of Horizon 2020 in 2020

as well as on progress towards achieving the digital targets, detailing the degree of Union progress in relation to the projected trajectories for each target, the assessment of the efforts necessary to achieve each target, including any investment gaps in digital capacities and innovation, as well as raising awareness about the actions needed to increase digital sovereignty in an open manner. The report should also include an assessment of the implementation of relevant regulatory proposals and an assessment of the actions undertaken at Union and Member States level."[29]

All European regulatory programs must be assessed periodically through a standardised process. Such assessment are essential to realise Union's plans to prioritise its own digital ecosystem and take the lead in establishing standards within the global digital landscape. These objectives can be achieved only by ensuring that its policies are implemented properly and achieve their targets. In its opinion on digital sovereignty as a crucial pillar for EU's digitalisation and growth, EESC has

"Already stressed the importance of digital sovereignty as a key pillar of Europe's economic, social and environmental development and has also stressed that this sovereignty must be based on global competitiveness and on strong cooperation between Member States. This is an essential precondition for the EU to become a global leader on the international scene, especially with regard to the reliability of digital technologies."[16]

Key Takeaway: Cooperation between Member States and impactful execution of EU's digital targets will help maintain its competitive advantage and global digital presence. Digital sovereignty seeks to ensure that European businesses and institutions lead in digital innovation while upholding high standards, enabling it to attract investment and cultivate international partnerships.

Competitive EU digital industries

EU has devised many policies around its digital Decade agenda that aims to build a globally competitive and resilient Europe. It includes digital targets focusing in strengthening the Union's capabilities towards digital skills, services, and infrastructure. It is set to guide the digital transformation of Europe. The working document on the implementation of the digital decade objectives and the digital rights and principles confirms that

"The Digital Decade objectives include notably the general objective to empower a more digitally sovereign, resilient, and competitive Union."[35]

Although building a more competitive EU is one of the major objectives of the digital decade programme, it relies heavily on European institutions' ability to innovate and secure its own digital ecosystem. One of the objectives is to set up European industrial bases and institutions which enable the development of innovative technologies inside Europe. In EESC's opinion, one such institution is ENISA, which aims to

"Support European digital sovereignty by developing a competitive European industrial base and reducing dependency on know-how developed outside the EU for key technology capabilities, provide technical exercises, workshops and even essential cyber hygiene training for professionals and non-professionals."[37]

Developing and promoting regional innovations is essential for the EU to build a competitive digital industrial and technological base but the Union must provide its critical sectors with technologies developed within the EU to promote regional innovation and maintain the resilience of essential services. It reduces risk and boosts the growth of industries and society. In the opininon on laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents,

"The EESC emphasises the vital aspect of procuring only Europe-based technology for equipping the EU Cybers Shield members with state-of-the-art technologies. The EU cannot afford to risk acquiring critical cyber technologies from foreign companies and it is

[37] Opinion of the European Economic and Social Committee on the 'Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) No 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")' (COM(2017) 477 final/2 2017/0225 (COD))

'in the EU's strategic interest to ensure that the Union retains and develops the essential capacities to secure its digital economy, society and democracy, to achieve full digital sovereignty as the only way to protect critical technologies, and to provide effective key cybersecurity services" [38]

While these measures may appear to pose challenges to global trade, they are vital for enhancing Europe's digital sovereignty and strengthening its digital industries. Enhancing EU-based technologies will not only grow digital industries in Europe but also lead to a more standardised digital market, increasing competitiveness. It is essential for maintain a strong position in the global digital market, especially for critical sectors such as defense and health as they handle highly sensitive data and are pivotal to national security and public well-being. In the annual report 2021 on the implementation of the common foreign and security policy, the European Parliament

"Underlines the need for the Union to further develop and strengthen its technological, operational and digital sovereignty and expertise through the enhancement of a strong European defence industry and market, the development of the European Defence Technological and Industrial Base, increased joint military research and development, procurement, training, maintenance, a common approach to security of supply, and a more ambitious cooperation with democratic allies." [39]

Key Takeaway: Competitive European industries are the pillars of a resilient economy and one of the main objectives of digital sovereignty. Strategies that strengthen EU's technological capabilities and provide oppurtunities to domestic businesses, not only help ensure Europe's strategic autonomy in the global digital landscape but also promote its vision of a digital single market.

4.3.4 Digital Single Market

Establishing a digital single market is among the prime agendas in EU's digital policies. It aims to enhance Europe's technological and industrial capabilities by unifying the national markets together to enhance its competitiveness in the global digital economy. With digital single market, EU seeks to evolve its strategic autonomy while boosting economic growth and innovation while empowering its citizens with equal opportunities.

Open and interoperable digital economy

Understanding the need to capture significant market share and position itself in the global digital space, the Union is promoting solutions that facilitate digital single market in Europe. It wants to compete with giant tech companies that capture a huge chunk of the market, making it difficult for smaller market to survive in cyberspace. The European Union's annual budget for the financial year 2024 affirms that

"Create more competition where compatible services and products could plug into systems surrounded by "walled gardens" and thus enable more companies to compete with digital gatekeepers. Therefore, it would contribute to European alternatives, European strategic autonomy and foster European digital sovereignty".[1]

Such interoperable digital solutions deliver economic sustainability by streamlining business operations as well as public administration. One concerning aspect for the Union to consider is that various European public administrations are increasingly reliant on foreign technologies and services. In an opinion on public sector interoperability, the EESC believes that

"EU public services should reduce their dependence on digital infrastructure provided by third countries, which jeopardises European digital sovereignty." [40]

[38] Opinion of the European Economic and Social Committee on 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services' (COM(2023) 208 final) — 2023/0108 (COD) and on 'Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents' (COM(2023) 209 final]) — 2023/0109 (COD)

[39] European Parliament resolution of 17 February 2022 on the implementation of the common foreign and security policy — annual report 2021 (2021/2182(INI))

[40] EUROPEAN ECONOMIC AND SOCIAL COMMITTEE 577TH PLENARY SESSION OF THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE, Opinion of the European Economic and Social Committee on the 'Proposal for a

Such solutions for cross-border and cross-sector services aid the eGovernance strategy being explored by the Union to ensure the resilience of public services and welfare programs. With the eGovernance strategy, EU is attempting to enhance interoperability across the public sector, contributing to a digitised society. The final evaluation of the ISA^2(Interoperability solutions for public administrations, businesses and citizens programme) affirms that

> "With the Tallinn Declaration on eGovernment , the ministers in charge of eGovernment policy across the EU spelled out their commitment to several principles, including 'interoperability by default'. This commitment was recently renewed by the Berlin Declaration on Digital Society and Value-Based Digital Government, which identified the need to take a value-based approach – incorporating digital sovereignty and interoperability – to the digital transformation of the public sector."[41]

However, to ensure 'interoperability by default', Europe needs to establish cooperation among its Member States as well as global partners. It needs to promote an open market with incentives to develop and operate interoperable solutions, building its strength in the digital markets. In its decision on the 2030 policy programme "Path to the Digital Decade", the European Council underlines

> "The need to enhance EU's digital sovereignty in a self-determined and open manner by building on its strengths and reducing its weaknesses and through smart and selective action, preserving open markets and global cooperation". [11]

An important aspect of open markets and global cooperation in the cyberspace is the standardisation of data management strategy, promoting innovative, interoperable digital solutions. The evaluation of the European Interoperability Framework (EIF), suggested the adoption of open specifications and standards, and

> "Given the EU's uniform approach to interoperability, the EIF may help ensure that standardisation initiatives support the European data strategy in line with the notion of digital sovereignty for Europe".[42]

Such a framework also encourages the usage of open-source software, promoting the 'interoperability by default' principle of the Union. To create an open and interoperable digital ecosystem that paves the way for a digital single market in Europe, open-source solutions are essential for connecting national systems and overcoming barriers. They also reinforce competitiveness and innovation. The European Union's annual budget for the financial year 2024 and the working document on impact assessment of the Interoperable Europe Act advocates that

> "Europe-wide capacity to strategically use and operationally deploy free and open source software (FOSS) is a cornerstone of strategies to achieve digital sovereignty, increased competitiveness of digital markets, innovation, and cybersecurity.[43]

> "Better support Open Source Software as a means to foster EU digital sovereignty and prevent vendor lock-in situations, for example by encouraging administrations to actively participate in existing international communities working on open source projects and open specifications."[13]

Interoperable solutions not only reduces its EU's reliance on large tech firms but also pave its way towards becoming an open digital economy. An open digital economy promotes harmonised standards to eliminate global barriers, encouraging collaboration across borders that create opportunities for all stakeholders while ensuring its own economic growth. In its conclusions on the cybersecurity of connected devices and of 25 March 2021, the European Council stresses that

---

Regulation of the European Parliament and of the Council laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act)' (COM(2022) 720 final – 2022/0379 (COD)) and on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a strengthened public sector interoperability policy – Linking public services, supporting public policies and delivering public benefits – Towards an "Interoperable Europe"'(COM(2022) 710 final)

[41]REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Results of the final evaluation of the ISA^2 programme

[42]COMMISSION STAFF WORKING DOCUMENT Final evaluation of the European Interoperability Framework (EIF) Accompanying the document Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act)

[43]footnote: budget2024-0207

"the European Union and its Member States need to ensure their digital sovereignty and strategic autonomy, while preserving an open economy."[44]

"the importance of the digital transformation for the Union's recovery, prosperity, security and competitiveness and for the well-being of our societies. It underlined the need to enhance EU's digital sovereignty in a self-determined and open manner by building on its strengths and reducing its weaknesses and through smart and selective action, preserving open markets and global cooperation."[45]

Key Takeaway: The digital transformation of the Union based on interoperable solutions and open digital economy reduces its technological dependencies and contributes in the establishing a digital single market for Europe. With digital sovereignty, the Union aims to develope an open digital economy, based on interoperable solutions while also collaborating with its strategic global partners.

Cooperation among key stakeholders

The establishment of a digital single market requires the development of frameworks that enhance cooperation among Member States, to achieve broader regulatory compliance and formulate unified industrial strategies. In the resolution on a civil liability regime for artificial intelligence, the European Parliament recommends the Commission

"to create a future-oriented and unified approach at Union level, setting common European standards for European citizens and businesses to ensure the consistency of rights and legal certainty throughout the Union and to avoid fragmentation of the Digital Single Market, which would hamper the goal of maintaining digital sovereignty, of fostering digital innovation in Europe and of ensuring a high-level protection of citizen and consumer rights, require that the liability regimes for AI-systems are fully harmonized." [17]

Additionally, building a digital single market requires the cooperation of numerous external strategic partners along with internal members. Collaborative strategic partnerships ensure Europe's competitiveness in the global digital markets, maintain resilience through diversified supply chains and reduced dependence on single actors, and boost innovation through collective research and development. In the 2030 Policy Programme 'Path to the Digital Decade', EESC highlights that

"digital sovereignty needs to be based on competitiveness that relies on solid cooperation between Member States, accompanied by the intrinsic involvement of civil society stakeholders, including businesses, workers, consumers, academia and other relevant stakeholders."[31]

Along with the cooperation among stakeholders, partnership between the private and public sectors is essential for maximizing the societal impact of technological innovation. It effectively bridges the digital divide and guarantees economic sustainability. By working together, the public and private sectors can ensure the resilience of their services while tackling complex challenges such as cybersecurity, contributing to their positioning in the global digital markets. The EU Policy on Cyber Defence uses similar strategies with the EESC supporting

"the extension of the mandate of the ECCC to support the activity of the EU Cyber Defence Coordination Centre. In addition, this network could support European digital sovereignty by developing a competitive European industrial base for key technological capabilities, based in part on work developed by contractual public-private partnerships (PPP). PPPs have proven to be the most effective approach to improving the cybersecurity of the entire digital ecosystem, but it cannot be unidirectional: public institutions must also share their intelligence with the private sector." [46]

Key Takeaway: Coordination among Key players and public-private partnership improves the competitiveness of the industrial base on Europe and improves the effectiveness of its digital strategies.

[44]Council conclusions on the cybersecurity of connected devices 2020/C 427/04

[45]COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT REPORT Accompanying the document Proposal for a Directive of the European Parliament and of the Council amending Directive 2014/53/EU on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment

[46]Opinion of the European Economic and Social Committee on the Joint Communication to the European Parliament and the Council: EU Policy on Cyber Defence (own initiative opinion)

public-private partnerships across all sectors is one of the primary intention behind digital sovereignty, enabling Europe to create a digital single market with its own technological capabilities.

4.3.5 Building own digital capacities

Supporting the development of European technologies and infrastructure is essential for achieving digital sovereignty and securing long-term resilience. Europe must determine its action towards building its own digital capabilities in telecommunication networks, data infrastructures, and key emerging technological innovations in artificial intelligence, quantum computing, and sustainable energy. It decreases dependence on external providers, reduces risks tied to geopolitical reliance, and protects its economic interests.

Development of European digital infrastructure

Europe seeks to achieve its sustainability goals while accelerating its digital transformation and fulfilling the demands of its growing digital economy. EU's push for climate-neutral digital technologies can be noticed in the report on setting out the requirements for accreditation, where it refers to the event

> "the State of the Union Address in September 2021, President von der Leyen underlined the need for Europe to shape its digital transformation and secure digital sovereignty. In this respect, the "2030 Digital Compass" laying down "the European way for the Digital Decade" provides for the uptake of digital skills and the development of climate-neutral and energy-efficient digital infrastructures." [47]

Energy-efficient digital infrastructures are essential for the EU's commitment to carbon neutrality. They not only significantly reduce operational costs but also drive innovation grounded in core European principles. A strong supply of semiconductor technologies is essential for driving technological advancements in digital infrastructures and guaranteeing the resilience of digital services. The communication 'Towards a more resilient, competitive and sustainable Europe' highlights the significant improvement in the Union's plan for securing the production and supply of semiconductors. It states that

> "since the proposal for the Chips Act by the Commission in February 2022, several companies have announced investments in semiconductor-related manufacturing facilities for a total amount of approximately EUR 100 billion. This will contribute to ensuring Europe's digital sovereignty and rebalancing global supply chains. The EU is also partnering with like-minded countries to work on semi-conductors." [48]

Ensuring the production and supply of semiconductor technologies in the EU directly impacts the development of critical infrastructures and technologies essential for maintaining Europe's strategic position in the global digital landscape. Digital infrastructures and technologies that are developed by European organisations serve as pivotal points in ensuring that the Union develops its own digital capacities. In an opinion on digital identity, data sovereignty, and the path to a just digital transition for citizens living in the information society, EESC put some specific comments on big data, stating that

> "EU digital sovereignty will be hard to achieve without its own EU digital tech giants, without storing European data on EU soil and without protection of these data from any extra-territorial access." [15]

Resilience of critical technologies and infrastructure ensured through the strengthening EU's own capacities reinforces its ability to safeguard societal and economic stability. In addition to critical technologies, the EU should promote innovation and establish provisions for the incorporation of advanced infrastructure, such as quantum computers, 6G networks, and the Internet of Things (IoT). The European Parliament and the Council underpin that a high-quality digital infrastructure

[47] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE on the implementation of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and repealing Regulation (EEC) No 339/93

[48] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Towards a more resilient, competitive and sustainable Europe

"can provide for innovative services, more efficient business operations, and smart, sustainable, digital societies while contributing to achieving the Union climate targets. It is of strategic importance to social and territorial cohesion and overall for the Union's competitiveness, resilience, digital sovereignty and digital leadership".[25]

Key Takeaway: The development of European digital infrastructure will enhance the production and innovation capacities of European industries, producing more opputunities and improving security. Promoting the development of cutting-edge infrastructures within Europe and building advanced technological capacities are leading objectives digital sovereignty.

Advance technological and digital capacities

In addition to focusing on expanding the technological development capacities in-house, one key area of concern for Europe is boosting the culture of innovation within the Union. It guarantees that Europe remains a dominant force in the race to excel in the global digital markets. The working document on the implementation of the Digital Decade objectives affirms that

"digital sovereignty covers among others the following elements: - The concrete means to ensure the resilience of the Union's digital supply chains; - The ability to innovate and develop digital technologies, services and infrastructures without being bound by design choices made elsewhere and that do not reflect our European values." [35]

Similarly, in the resolution on civil liability regime for artificial intelligence, the European Parliament considers that

"Union will only achieve the objectives of maintaining the Union's digital sovereignty and of boosting digital innovation in Europe with consistent and common rules in line with a culture of innovation".[17]

EU should focus a culture of innovation to develop digital technologies that reflect its values and principles. To create the said culture of innovation, the Union needs to promote start-ups and SMEs that committed to innovation in Europe. Start-ups and SMEs that actively foster a culture of innovation in Europe are not just shaping the future, they are leading the charge in developing groundbreaking products and solutions. This momentum attracts top global talent and significant investment, solidifying EU's role as a key player in the global market. In its opinion on Digital Sovereignty, the EESC acknowledges

"The key role played by small and medium sized enterprises (SMEs) in shaping the EU's digital sovereignty, especially through their interactions with large EU tech companies."[16]

They encourage collaboration while boosting the adoption of emerging technologies, particularly by enhancing Europe's digital and cloud capacities. As the global technology sector adopts cloud technologies, the EU should seek to develop solutions that enhance its capabilities in advance technologies. Most cloud and data storage solutions are provided by companies outside Europe due to the limited capacity of the European tech industry. EESC affirms this in the same communication which provides its opinion on digital sovereignty, where it supports calls for

"The EU to develop a cloud and data infrastructure to build its digital sovereignty and address the huge imbalance of the cloud and data storage market being almost totally dominated by non-EU companies."[16]

The EU can address the dominance of foreign companies in cloud and data infrastructure by building its own digital capabilities. Such capabilities can be built through investments in emerging technologies that drive innovation in global digital markets. The working document on Country Report Germany 2019 argues that

"Investment in artificial intelligence and cybersecurity is needed if Germany is to remain globally competitive and safeguard digital sovereignty."[49]

[49]COMMISSION STAFF WORKING DOCUMENT Country Report Germany 2019 Including an In-Depth Review on the prevention and correction of macroeconomic imbalances Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN CENTRAL BANK AND THE EUROGROUP 2019 European Semester: Assessment of progress on structural reforms, prevention and correction of macroeconomic imbalances, and results of in-depth reviews under Regulation (EU) No 1176/2011

One of EU's key priorities for investment is in interdisciplinary research and innovation. Europe is providing various funding mechanisms to develop new technologies through various multi-country initiatives and programs such as Horizon Europe, Digital Europe, IvestEU among others. This is inline with the working document on Annual Single Market Report 2021 and resolution on the Digital future of Europe endorsing for

> "investments in high-impact multi-country projects in critical technological areas will enable the deployment of large digital infrastructures, capabilities and production capacities that will enhance European digital sovereignty and underpin the digital transformation of all sectors, with important spill-overs for the EU economy."[50]

> "investing in sciences, research, and development in the areas of digital and AI, fostering better access to venture capital, developing a strong cybersecurity of critical infrastructures and electronic communication networks and access to unbiased, high-quality data are the cornerstones of ensuring the digital sovereignty of the Union".[34]

With investments in multi-country projects, EU aims to advance its technological capabilities and production capacities within its new industrial startegy. Investment in research and innovation aim to enhance competitiveness, build its strategic capacities that drive economic growth, and address societal and environmental challenges. In the working document on the decision to establish the 2030 Policy Programme, the European Parliament and the Council describe that

> "industry stakeholders strongly supported the ambition to achieve digital sovereignty by expanding European production capacities through independent research and industry activities, especially regarding semiconductors"[11]

Key Takeaway: While digital sovereignty aims to achieve digital independence, increase competitiveness and enhance global cooperation by focusing on research and innovation, skilled labor in the digital domain is essential. It emphasises on the significant attention required towards provisioning of digital skills in Europe, through education and training.

Provision for digital skills through education and training

Europe must prioritise the development of the digital and cyber skills of its workforce and institutions, empowering them to confidently navigate and excel in the digital age. In the working document of the report on the state of the Digital Decade 2023, some cardinal points are described among which one aspect stresses that

> "There is no digital future without the appropriate digital skills. Without the right digital skills, the European Union will not be able to cope with current and future strategic dependencies. Only by stepping up efforts in boosting digital skills and the number of ICT specialists, the EU will continue to be able to master the rapid evolution of digital technologies and to ensure its digital sovereignty."[51]

The significant digital skills gap in the Union is hindering its digital progress and necessitating the need for digital education and training within the Union. While digital education is essential for closing the skills gaps necessary for technological innovation and cybersecurity, the Union must regulate its education system, which is influenced by large corporations. In the working document on improving the provision of digital skills in education and training, the Council

> "indicates a tension between public education systems and private entities, particularly EdTech and large technology corporations. We saw under this topic the concept of digital sovereignty to protect against the influences of 'tech giants', and suggestions to develop an alternative teaching and learning platform for digital education and skills."[52]

[50] COMMISSION STAFF WORKING DOCUMENT Annual Single Market Report 2021 Accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Updating the 2020 New Industrial Strategy: Building a stronger Single Market for Europe's recovery

[51] COMMISSION STAFF WORKING DOCUMENT Digital Decade Cardinal Points Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Report on the state of the Digital Decade 2023 52023SC0571

[52] COMMISSION STAFF WORKING DOCUMENT Accompanying the documents Proposal for a Council Recommendation on the key enabling factors for successful digital education and training Proposal for a Council Recommendation on improving the provision of digital skills in education and training

Key Takeaway: Europe needs to counter the influence of the 'EdTech' giants by developing alternative EU-based platforms for digital education and training curated for upskilling an reskilling its workforce. It will help achieve the objective of digital sovereignty of security and resilience of European industries in cyberspace by enhancing the digital and cyber skills of the workforce, through education and training.

4.3.6 Cybersecurity and resilience

Cybersecurity and resilience of EU's critical entities is a key pillars for the Union's transition towards digital sovereignty. For safeguarding information flow and maintaining the operational integrity, robust cybersecurity measures are essential. The security standards and comprehensive frameworks implementing advanced threat detection, paired with resilient response protocols, are essential for the protection of technologies and infrastructures of Europe.

Strengthen cybersecurity and defence capabilities

To create a safer digital ecosystem and safeguard the resilience of critical technologies and services in the rapidly evolving cyberspace, the EU needs to enhance its cybersecurity and defence capabilities. The resolution on the state of EU cyber defence capabilities and the communication on EU Policy on Cyber Defence, argue that

> "Data encryption and the enhancement and widest possible use of such capabilities can make a significant contribution to the cyber security of states, societies and industry; encourages a 'European digital sovereignty' programme in order to foster and enhance the current capabilities in terms of cyber and encryption tools inspired by fundamental European rights and values such as privacy, freedom of expression and democracy, with the aim of enhancing European competitiveness in the cybersecurity market and boosting internal demand" [53]

> "EU must ensure its technological and digital sovereignty in the cyber field. The EU's capacity to act will depend on its ability to master and develop cutting edge technologies for cybersecurity and cyber defence in the EU. As cyber technologies have a strong dual-use potential, the cybersecurity and cyber defence industries, research and development, and innovation activities must work in a much more synergetic manner to develop better capabilities."[54]

The security and defense capabilities must be strengthened in alignment with cybersecurity standards that are constantly evolving to address emerging risks and threats. To build proper cybersecurity and defence capabilities, it is essential to master cutting-edge technologies and consistently upgrade to incorporate information new threats and vulnerabilities. In the working documents on improving the provision of digital skills in education and training, the EESC supports

> "the proposal to create a cybersecurity competence network. This network would be sustained by a Cybersecurity Research and Competence Centre (CRCC). This network could support European digital sovereignty by developing a competitive European industrial base for key technology capabilities based on the work done by the contractual Public-Private Partnership (cPPP), which should evolve into a Tripartite Joint Undertaking."[37]

Key Takeaway: A cybersecurity competence network reinforced through public-private partnership will bring together best experts and resources to improve the resilience of cyberspace and develop a competitive base. It will also foster innovation and help reduce reliance on foreign cybersecurity solutions by European industry. A cybersecurity competence network creates a coordinated approach to achieve digital sovereignty, protecting the Union's digital technologies and infrastructure..

Protection of technologies and infrastructure

[53] European Parliament resolution of 7 October 2021 on the state of EU cyber defence capabilities (2020/2256(INI))

[54] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL EU Policy on Cyber Defence

Most of the digital technologies rely on semiconductor chips or materials. Ensuring the resilence of production and supply of semiconductor technologies plays a crucial role in Europe's economic growth and digital stability. Collaborative research and innovation in the semiconductor field are essential for ensuring digital sovereignty. In the resolutions on Chips Joint Undertaking under Horizon Europe and Global approach to research and innovation: Europe's strategy for international cooperation in a changing world, the European Parliament advocates that

> "reinforcing Europe's semiconductor ecosystem is one of the key components to achieving economic resilience and security, strategic autonomy, enhanced digital sovereignty and reduced dependencies; and will play an important role in the green and digital transitions".[55]

> "the crucial role of semiconductors in ensuring the digital sovereignty of the Union; welcomes the Commission's initiatives in this regard and highlights the collaboration on research with third countries associated with existing Union programmes".[56]

Given the importance of the semiconductor ecosystem on resilience in the production and innovation of digital technologies, the discussions on digital sovereignty in this context in EU policies are essential for its digital future. Secure and accessible digital infrastructures in the EU ensure that its digital transformation safeguards operational resilience for businesses and public administration and enables economic resilience, security, and reliability. In the decision to establish the Digital Decade Policy Programme 2030, the European Parliament and the Council advocated for

> "ensuring the Union's digital sovereignty in an open manner, in particular by secure and accessible digital and data infrastructures capable of efficiently storing, transmitting and processing vast volumes of data that enable other technological developments, supporting the competitiveness and sustainability of the Union's industry and economy, in particular of SMEs, and the resilience of the Union's value chains, as well as fostering the start-up ecosystem and the smooth functioning of the European digital innovation hubs.'[29]

Ensuring the security and accessibility of digital infrastructures minimises the risk of disruptions against critical services, which is crucial for public safety and economic stability. Critical infrastructure and technologies underpin the functioning of European society, economy, and the security of its member states, making it essential to cultivate strategies for its security and stability. In its opinion on EU Policy on Cyber Defence, EESC considers it to be

> "in the EU's strategic interest to ensure that the Union retains and develops the essential capacities to secure its digital economy, society and democracy, to achieve full digital sovereignty as the only way to protect critical technologies and to provide effective key cybersecurity services."[46]

Thus, protection against disruptions in critical infrastructures such as healthcare systems, energy grids, transportation, and water supply is essential as it can lead to societal and economic challenges. EU needs to develop platforms that cultivate trustworthy media and information to counter misleading news, ensuring the integrity of public discourse and protecting democratic values. The European Union's general budget for the financial year 2022, addresses this concern

> "with a view to contributing to Europe's digital sovereignty and to a European Public Sphere, this preparatory action adapts existing technological means and further develops solutions to create a platform capable of improving European citizens' access to trusted information from across Europe."[21]

Key Takeaway: As social media platforms gain more influence, trust in media is declining, with conflicting information circulating rapidly from various sources. One of the aims of the EU with digital sovereignty is to curb the influence of the platforms and build its own trustworthy media platforms to enhance its capacity and improve security. By supporting EU-based trustworthy media platforms, Europe reduces its dependency on external giant cooperatives, building a resilient, informed society that aligns with its core values and principles.

[55]European Parliament legislative resolution of 15 February 2023 on the proposal for a Council regulation amending Regulation (EU) 2021/2085 establishing the Joint Undertakings under Horizon Europe, as regards the Chips Joint Undertaking (COM(2022)0047 — C9-0113/2022 — 2022/0033(NLE))

[56]European Parliament resolution of 6 April 2022 on a global approach to research and innovation: Europe's strategy for international cooperation in a changing world (2021/3001(RSP)

5 Conclusion

The notion of *digital sovereignty* within the EU emerges as a significant geopolitical concern[Fabbrini et al., 2020]. Many researchers have tried to understand this term with the help of both political and academic literature, we analyse what the European Union means by digital sovereignty in its legal documents by exploring the motivations behind the push and the goals it seeks to achieve. To answer our first sub-question, we establish that that EU's motivation for digital sovereignty is grounded in addressing crucial issues and challenges such as foreign digital dependencies, a lack of a common governance framework, insufficient cybersecurity, and the growing impact of technology on Europe's social and economic growth.

To answer our second sub-question, we establish that EU has several strategic goals to address these challenges, including enhancing data control, a democratic digital transformation, achieving open strategic autonomy, fostering a digital single market, building its own digital capacities, and ensuring cybersecurity and resilience. With these goals, the EU intends to secure its position as a global leader by setting digital standards while safeguarding European values of inclusion, fairness, and respect for fundamental rights.

5.1 Understanding Digital Sovereignty

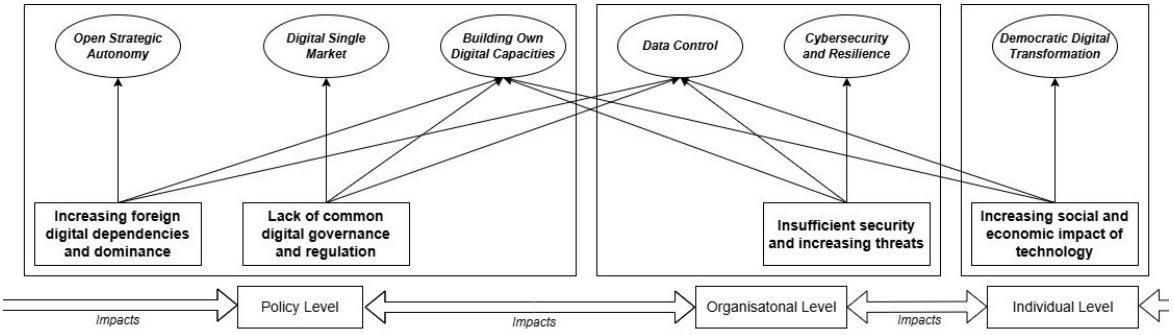

Figure 6: Visual illustration of the theoretical relationship between the motivation and goal of digital sovereignty across various levels

Figure 6 illustrates a relational diagram between different motivations of digital sovereignty with its goals. To establish a theoretical connection for these relationships, we categorize them at different levels based on their expected impact.

- At the policy level, structural challenges such as governance, regulation, and international dependencies are addressed through the goals of open strategic autonomy, a digital single market, and building own digital capacities. These goals are interdependent and contribute to each other's progress but are highly influenced by European policies and governance decisions. This relationship is evident from EU's attempt to regulate and unify it's markets with legislative approaches such as DMA (Digital Markets Act) and DSA (Digital Services Act).

- At the organisational level, the focus shifts towards the increasing threats and security risks faced by the EU, tackled by the EU's goal of data control and enhancing cybersecurity and resilience. The objective is to ensure businesses operate securely and innovation is not hindered within the EU's digital ecosystem. Both these goals are interdependent and rely on the organisational posture in cyberspace. To safeguard digital infrastructures and data, EU provides guidelines and requirements to organisations through GDPR(General Data Protection Regulation) and NIS2 (Network and Information Systems) Directive, enhancing the security and resilience of cyberspace.

- At the individual level, the challenge is the increasing impact of digital technologies on European society and economy. This impact can be limited by ensuring that Europe's digital transformation follows democratic principles and that technology benefits citizens equitably, fostering trust, inclusion, and participation in the digital economy. By utilising the eIDAS(electronic Identification, Authentication, and Trust Services) regulation alongside GDPR(General Data Protection Regulation) protections, interoperability in the European digital space will be established while safeguarding the values and principles of the Union.

Among the six dimensions of the EU concerning digital sovereignty, building its own digital capacities and data control contribute to most of the challenges that the EU wants to overcome in its digital economy, making them crucial aspects of digital sovereignty. This multi-level approach provides a holistic vision of the EU regarding digital sovereignty, aiming to ensure that technological developments align with its democratic, strategic, and economic priorities.

The EU's vision of digital sovereignty is not merely about positioning itself as a competitive and autonomous player in the global digital landscape and reducing dependencies on foreign actors but about fostering a secure, innovative, and inclusive digital ecosystem based on its foundational values. Digital sovereignty for the European Union is about building its strategic capabilities through standardised and interoperable digital solutions, a unified digital market and a common governance model.

5.2 Limitations and Future Work

While this study provides valuable insights into the concept of digital sovereignty, we identify a few points that can used as starting points for future research. A primary constraint is in the limited scope of documents analysed; of the 79 examined, few explicitly define this concept or elaborate on its meaning and motivations. We only considered text in this analysis that explicitly referred to digital sovereignty; as a next step, researchers can make use of topic detection algorithms to identify similar goals and contribute to the broader understanding of its complementary goals.

Additionally, while qualitative analysis is significant for identifying recurring themes, it may oversimplify complex relationships due to subjective interpretations inherent in the Gioia method. The focus on EU policy documents introduces potential bias, as perspectives from other geopolitical contexts, such as the U.S., Australia, or the U.K., were not explored.

References

L. Amoore and M. de Goede. *Risk and the War on Terror (1st ed.)*. Routledge, 2008. doi: https://doi.org/10.4324/9780203927700.

Rozalia Beica. Enabling information age through advanced packaging technologies and electronic materials. In *2018 Pan Pacific Microelectronics Symposium (Pan Pacific)*, pages 1–5, February 2018. doi: 10.23919/PanPacific.2018.8318733. URL https://ieeexplore.ieee.org/document/8318733/?arnumber=8318733.

Rocco Bellanova, Helena Carrapico, and Denis Duez. Digital/sovereignty and european security integration: An introduction. *European Security*, 31(3):337–355, July 3 2022. doi: 10.1080/09662839.2022.2101887. URL https://doi.org/10.1080/09662839.2022.2101887.

Annegret Bendiek and Matthias C Kettemann. Revisiting the eu cybersecurity strategy: A call for eu cyber diplomacy. 2021. URL https://www.swp-berlin.org/10.18449/2021C16/.

Didier Bigo. The (in)securitization practices of the three universes of eu border control: Military/navy – border guards/police – database analysts. *Security Dialogue*, 45(3):209–225, 2014. doi: 10.1177/0967010614530459. URL https://doi.org/10.1177/0967010614530459.

Blancato. The cloud sovereignty nexus: How the european union seeks to reverse strategic dependencies in its digital ecosystem, 2024a. URL https://onlinelibrary.wiley.com/doi/10.1002/poi3.358.

Filippo Gualtiero Blancato. The cloud sovereignty nexus: How the European Union seeks to reverse strategic dependencies in its digital ecosystem. *Policy & Internet*, 16(1):12–32, 2024b. ISSN 1944-2866. doi: 10.1002/poi3.358. URL https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.358. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/poi3.358.

F. Bostoen. Understanding the digital markets act. *The Antitrust Bulletin*, 68(2):263–306, 2023. doi: 10.1177/0003603X231162998. URL https://doi.org/10.1177/0003603X231162998.

Anu Bradford. *Digital empires: The global battle to regulate technology*. Oxford University Press, 2023.

Thierry Breton. Speech by commissioner thierry breton at hannover messe digital days, July 2020. URL https://ec.europa.eu/.

Dennis Broeders, Fabio Cristiano, and Monica Kaminska. In search of digital sovereignty and strategic autonomy: Normative power europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, 61(5):1261–1280, 2023a. doi: 10.1111/jcms.13462. URL https://doi.org/10.1111/jcms.13462.

Dennis Broeders, Fabio Cristiano, and Monica Kaminska. In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. *JCMS: Journal of Common Market Studies*, 61(5):1261–1280, 2023b. ISSN 1468-5965. doi: 10.1111/jcms.13462. URL https://onlinelibrary.wiley.com/doi/abs/10.1111/jcms.13462. _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/jcms.13462.

Randolph Luca Bruno, Julia Korosteleva, Kirill Osaulenko, and Slavo Radosevic. Sectoral digital capabilities and complementarities in shaping young firms' growth: evidence from Europe. *Entrepreneurship & Regional Development*, 36(1-2):115–135, January 2024. ISSN 0898-5626, 1464-5114. doi: 10.1080/08985626.2023.2218314. URL https://www.tandfonline.com/doi/full/10.1080/08985626.2023.2218314.

Anupam Chander and Haochen Sun. Sovereignty 2.0. *Georgetown Law Faculty Publications and Other Works*, 2404, 2021. doi: 10.2139/ssrn.3904949. URL https://ssrn.com/abstract=3904949. University of Hong Kong Faculty of Law Research Paper No. 2021/041.

Stephane Couture and Sophie Toupin. What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, 21(10):2305–2322, 2019. doi: 10.1177/1461444819865984. URL https://doi.org/10.1177/1461444819865984.

Ashis Dutta and Kevin McCrohan. Management's role in information security in a cyber economy. *California Management Review*, 45(1):67–87, 2002. doi: 10.2307/41166154. URL https://doi.org/10.2307/41166154.

Federico Fabbrini, Edoardo Celeste, and John Quinn. *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*. Hart Publishing, 2020. ISBN 978-1-5099-4066-0 978-1-5099-4068-4 978-1-5099-4067-7 978-1-5099-4069-1. doi: 10.5040/9781509940691.

T. Fiorito, R. Hoff, and M. Ehrenhard. The influence of critical events on the social control of misconduct: Regulatory enforcement in the european banking industry. In C. Gabbioneta, M. Clemente, and R. Greenwood, editors, *Organizational Wrongdoing as the "Foundational" Grand Challenge: Definitions and Antecedents*, volume 84 of *Research in the Sociology of Organizations*, pages 51–72. Emerald Publishing Limited, Leeds, 2023. doi: 10.1108/S0733-558X20230000084003. URL https://doi.org/10.1108/S0733-558X20230000084003.

Christopher Foster and Shamel Azmeh. Latecomer economies and national digital policy: An industrial policy perspective. *Journal of Development Studies*, 56(7):1247–1262, November 2019. ISSN 0022-0388. doi: 10.1080/00220388.2019.1677886.

Patrick W Franzese. Sovereignty in cyberspace: Can it exist. *AFL Rev.*, 64:1, 2009.

Dennis A. Gioia, Kevin G. Corley, and Aimee L. Hamilton. Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods*, 16(1):15–31, January 2013. ISSN 1094-4281, 1552-7425. doi: 10.1177/1094428112452151. URL https://journals.sagepub.com/doi/10.1177/1094428112452151.

Paul Grant. TECHNOLOGICAL SOVEREIGNTY: FORGOTTEN FACTOR IN THE 'HI-TECH' RAZZAMATAZZ. *Prometheus*, 1(2):239–270, 1983. doi: 10.1080/08109028308628930. URL https://doi.org/10.1080/08109028308628930.

Harald Gruber. Innovation, skills and investment: a digital industrial policy for Europe. *Economia e Politica Industriale*, 44(3):327–343, September 2017. ISSN 0391-2078, 1972-4977. doi: 10.1007/s40812-017-0073-x. URL http://link.springer.com/10.1007/s40812-017-0073-x.

Malte Hellmeier and Franziska von Scherenberg. A Delimitation of Data Sovereignty from Digital and Technological Sovereignty. *ECIS 2023 Research Papers*, 1(2), 2023. URL https://aisel.aisnet.org/ecis2023_rp/306.

Cristian Hesselman, Paola Grosso, Ralph Holz, Fernando Kuipers, Janet Hui Xue, Mattijs Jonker, Joeri de Ruiter, Anna Sperotto, Roland van Rijswijk-Deij, Giovane C. M. Moura, Aiko Pras, and Cees de Laat. A Responsible Internet to Increase Trust in the Digital World. *Journal of Network and Systems Management*, 28(4):882–922, October 2020. ISSN 1064-7570, 1573-7705. doi: 10.1007/s10922-020-09564-7. URL https://link.springer.com/10.1007/s10922-020-09564-7.

Patrik Hummel, Matthias Braun, Max Tretter, and Peter Dabrock. Data sovereignty: A review. *Big Data & Society*, 8(1):2053951720982012, January 1 2021. doi: 10.1177/2053951720982012. URL https://doi.org/10.1177/2053951720982012.

Caroline Humphrey. Sovereignty. *A Companion to the Anthropology of Politics*, pages 418–436, 2007.

Bernardus Jansen, Natalia Kadenko, Dennis Broeders, Michel Van Eeten, Kevin Borgolte, and Tobias Fiebig. Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, 40(4):101862, October 2023. ISSN 0740624X. doi: 10.1016/j.giq.2023.101862. URL https://linkinghub.elsevier.com/retrieve/pii/S0740624X2300062X.

G. Javadian, C. Dobratz, A. Gupta, V.K. Gupta, and J.A. Martin. Qualitative research in entrepreneurship studies: A state-of-science. *The Journal of Entrepreneurship*, 29(2):223–258, 2020. doi: 10.1177/0971355720930564. URL https://doi.org/10.1177/0971355720930564.

Daniel Lambach and Kai Oppermann. Narratives of digital sovereignty in German political discourse. *Governance*, 36(3):693–709, 2023. ISSN 1468-0491. doi: 10.1111/gove.12690.

N. Leemann and D.K. Kanbach. Toward a taxonomy of dynamic capabilities – a systematic literature review. *Management Research Review*, 45(4):486–501, 2022. doi: 10.1108/MRR-01-2021-0066. URL https://doi.org/10.1108/MRR-01-2021-0066.

Jenny Leonard, Debby Wu, and Katrina Manson. Taiwan tensions spark new round of us wargaming on risk to tsmc, 10 2022. URL https://www.bloomberg.com/news/articles/2022-10-07/taiwan-tensions-spark-new-round-of-us-war-gaming-on-risk-to-tsmc.

I.J. Lloyd. *Information Technology Law*. Butterworths, 1993. ISBN 0406024464, 978-040602446-6. URL https://www.scopus.com/inward/record.uri?eid=2-s2.0-85041145916&partnerID=40&md5=39c35af039f8c9acd3d7bbe31cddb29b.

Arlette Meiring, Svetlana Yakovleva, Kristina Irion, Joris van Hoboken, and van Eechoud. *Information Law and the Digital Transformation of the University. Part I. Digital Sovereignty*. Institute for Information Law, Amsterdam, September 2023.

Angela Merkel. Speech by Federal Chancellor Dr Angela Merkel opening the 14th Annual Meeting of the Internet Governance Forum in Berlin on 26 November 2019. November 2019. URL https://www.intgovforum.org/en/content/german-chancellors-remarks-to-the-igf-2019.

Linda Monsees and Daniel Lambach. Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, 31(3):377–394, July 2022. ISSN 0966-2839, 1746-1545. doi: 10.1080/09662839.2022.2101883. URL https://www.tandfonline.com/doi/full/10.1080/09662839.2022.2101883.

Milton L. Mueller. *Networks and States: The Global Politics of Internet Governance*. The MIT Press, September 2010. ISBN 978-0-262-28966-5. doi: 10.7551/mitpress/9780262014595.001.0001. URL https://doi.org/10.7551/mitpress/9780262014595.001.0001.

Milton L Mueller. Against Sovereignty in Cyberspace. *International Studies Review*, 22(4):779–801, September 2019. ISSN 1521-9488. doi: 10.1093/isr/viz044. URL https://doi.org/10.1093/isr/viz044. _eprint: https://academic.oup.com/isr/article-pdf/22/4/779/34544628/viz044.pdf.

Francesca Musiani. Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*, 25(6):785–800, 2022. doi: 10.1080/1369118X.2022.2049850. URL https://doi.org/10.1080/1369118X.2022.2049850.

Medina-López A. Ménez-Partearroyo, M. and S. Rana. Business intelligence and business analytics in tourism: insights through gioia methodology. *International Entrepreneurship and Management Journal*, 20:2287–2321, 2024. doi: 10.1007/s11365-024-00973-7. URL https://doi.org/10.1007/s11365-024-00973-7.

Andreas Osiander. Sovereignty, international relations, and the westphalian myth. *International Organization*, 55(2):251–287, April 2001. doi: 10.1162/00208180151140577. URL https://doi.org/10.1162/00208180151140577.

Vítor Pedreira, Daniel Barros, and Pedro Pinto. A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. *Sensors*, 21(15):5189, July 2021. ISSN 1424-8220. doi: 10.3390/s21155189. URL https://www.mdpi.com/1424-8220/21/15/5189.

Daniel Philpott. Sovereignty: an introduction and brief history. *Journal of International Affairs*, 48(2): 353–368, 1995. URL https://link.gale.com/apps/doc/A16714038/AONE?u=anon~edcd28fd&sid=googleScholar&xid=34a29178. Accessed 16 July 2024.

Rupprecht Podszun. Digital Ecosystems, Decision-Making, Competition and Consumers – On the Value of Autonomy for Competition. *SSRN Electronic Journal*, 2019. ISSN 1556-5068. doi: 10.2139/ssrn.3420692. URL https://www.ssrn.com/abstract=3420692.

Julia Pohle and Thorsten Thiel. Digital sovereignty. *Internet Policy Review*, 9(4), December 2020. ISSN 2197-6775. doi: 10.14763/2020.4.1532. URL https://policyreview.info/concepts/digital-sovereignty.

Marietje Schaake and Mathias Vermeulen. Towards a values-based European foreign policy to cybersecurity. *Journal of Cyber Policy*, 1(1):75–84, January 2016. ISSN 2373-8871, 2373-8898. doi: 10.1080/23738871.2016.1157617. URL http://www.tandfonline.com/doi/full/10.1080/23738871.2016.1157617.

R. Schaller. Technological innovation in the semiconductor industry: A case study of the International Technology Roadmap for Semiconductors (ITRS). In *PICMET '01. Portland International Conference on Management of Engineering and Technology. Proceedings Vol.1: Book of Summaries (IEEE Cat. No.01CH37199)*, volume 1, pages 195 vol.1–, July 2001. doi: 10.1109/PICMET.2001.951917. URL https://ieeexplore.ieee.org/document/951917/?arnumber=951917.

Timo Seidl and Luuk Schmitz. Moving on to not fall behind? technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy. *Journal of European Public Policy*, 0(0):1–28, 2023. doi: 10.1080/13501763.2023.2248204. URL https://doi.org/10.1080/13501763.2023.2248204.