UNIVERSITÀ DEGLI STUDI DI PADOVA

DEPARTMENT OF POLITICAL SCIENCE, LAW, AND INTERNATIONAL STUDIES

Master's Degree in European and Global Studies

Constructing Digital Sovereignty in the Cyber Age: A Comparative Analysis of the EU and India's Strategic Autonomy and the Role of the Trade and Technology Council

Supervisor: Prof. Claudia Padovani

Candidate: Jovan Nikolic

Matriculation No. 2071483

A.Y. 2024/2025

Abstract (300 WORDS)

This study examines the role of the EU-India Trade and Technology Council (TTC) as a discursive space where digital sovereignty is negotiated, contested, and, in some areas, aligned. Using a constructivist approach and political discourse analysis, the research investigates how the European Union (EU) and India conceptualize, operationalize, and articulate digital sovereignty within the TTC. By analyzing policy documents, official statements, and ministerial outcomes, the study identifies convergence in AI and semiconductor cooperation, where digital sovereignty is framed as a tool for strategic autonomy and technological resilience. Conversely, divergences in data governance and cybersecurity persist due to fundamentally different sovereignty claims—the EU favors regulatory control and global interoperability, while India prioritizes state-driven digital nationalism and security-focused policies. The findings suggest that digital sovereignty is not a fixed concept but an evolving discourse shaped by institutional negotiations and geopolitical pressures. The TTC serves both as a mechanism for policy coordination and a structured arena for sovereignty contestation, allowing the EU and India to maintain strategic engagement despite regulatory divergences. However, the study also reveals limitations in the TTC's ability to harmonize sovereignty claims in deeply contested areas, such as cross-border data flows and cybersecurity governance.

Table of Contents

Abstract (300 WORDS) **2**

Table of Contents **3**

LIST OF ACRONYMS **5**

1. Introduction **6**

2. Constructing Statehood in the Cyber Age **11**

2.1. How norms, ideas, and discourse shape international politics 11

2.2. Speech Act Theory 15

2.3. Sovereignty 16

2.3.1. Westphalian Sovereignty Decline 17

2.3.2. Constructivist Rethinking of Sovereignty 19

2.3.3. Digital Sovereignty 20

2.3.4. The Development of Alternative Discourses 24

2.4. Digital Sovereignty in the EU - Overview 27

2.4.1. Discourse Analysis Approach 28

2.4.2. Theoretical Approaches to Digital Sovereignty Analysis 33

3. Research Design and Methodology **34**

4. The EU-India Relations in the Digital Age **40**

4.1. Historical Overview of EU-India Relations 40

4.2. Strengthening the Partnership (2000-2013) 41

4.2.1. BTIA and the Emergence of Trade Issues (2007-2013) 44

4.3. Attempts to Put Negotiations Back on Track (2014-2022) 47

4.3.1. Common Denominator: Strategic Autonomy 48

4.4. Toward a Digital Partnership: New Dimensions in EU-India Relations 50

4.4.1. Mutual Interests and Diverging Views in the EU-India Relations 52

4.4.2. Open Questions - The Road to TTC 56

4.5. The EU-India Trade and Technology Council (TTC) 57

4.5.1. TTC, Digital Sovereignty and Constructivist Theory 57

4.5.2. The Structure of the TTC and Ministerial Meetings 58

5. Comparative Digital Sovereignty Analysis in the EU-India Relations 61

5.1. The EU Digital Sovereignty Documents Analysis 61

5.2. The Digital Sovereignty in the EU - Recap 80

5.3. Digital Sovereignty of India Documents Analysis 84

5.4. The Digital Sovereignty in India - Recap 98

6. TTC and the Convergence and Divergence of Digital Sovereignty Discourses 102

6.1. The EU-India Comparison 102

6.2. Convergence 106

6.3. Divergence 107

7. Concluding Remarks 109

References 112

LIST OF ACRONYMS

EU	European Union
US	United States
TTC	Trade and Technology Council
AI	Artificial Intelligence
IoT	Internet of Things
ICT	Information and Communications Technology
GAFAM	Google, Amazon, Facebook, Apple, Microsoft
BATX	Baidu, Alibaba, Tencent, Xiaomi
NSA	National Security Agency
ITU	International Telecommunication Union
ICANN	Internet Corporation for Assigned Names and Numbers
KPIs	Key Performance Indicators
OECD	Organization for Economic Cooperation and Development
PDA	Policy Discourse Analysis
WTO	World Trade Organization
WCIT	World Conference on International Communications
EC	European Commission
IGF	Internet Governance Forum
IR	International Relations

1. Introduction

On 23rd of April 2024, the US Senate passed a law that would force a sale of TikTok by its Chinese owner or ban it due to national security concerns and risks that the Chinese government would gain access to data of 170 million US users of the platform (Maheshwari & McCabe, 2024). During the hearing of TikTok's CEO, Shou Zi Chew, the solution for the ongoing concerns of the US government was the so-called Project Texas. This project was based on storing the data of US citizens on the US territory ensuring that, according to the words of Chew:" American data stored on American soil overseen by American companies by American personnel" (Clayton, 2023).

The latest ban on US-TikTok dynamics is just the peak of an iceberg in which governments worldwide are trying to regain control over digital spaces. During the COVID-19 pandemic, the UK government failed to introduce a mobile app to track the number of infected people because of the impossibility of developing the app outside of a system operated by Google and Apple (Burgess, 2020). In the last 5 years, the Indian government banned more than 50 Chinese apps to protect Indian sovereignty (Mehrotra, 2022). Under the current European Commission (EC), digital sovereignty is one of the core principles of the EU digital strategy (Burwell & Propp, 2022).

As the efforts to regain control over digital spaces are piling up, the international system is entering into arguably one of the most challenging periods since the years that led up to the Cuban Missile Crisis (Blackwill, 2024). With crisis points such as the war in Eastern Europe and the Israeli offensive in the Gaza Strip, diplomacy is yet to mitigate the danger stemming from these cases showing that the liberal world order is gradually eroding. On the other hand, the US-China relations are on a path to confrontation as the newly emerging balance of power in Asia is shifting against the interest of the US (Ibidem). On the contrary, the EU and India are in danger of being sidelined and lacking any decision-making influence on the important issues of international politics (Müller-Brandeck-Bocque et al., 2021, p. 5).

Not only have international politics become increasingly volatile and full of tensions but, at the same time, more complex. More precisely, the tech and digital sector has become the center of geopolitical tensions as this sector has been perceived probably as

the most important arena for state competition and power struggles (Christakis, 2020, p. 42). In other words, whoever runs the global Internet of Things (IoT) and excels at AI and Machine Learning will have a geostrategic advantage (Ibidem). However, the expansion of the digital sector and advanced technologies has been captured by a handful of actors, namely big tech companies that are seen as the main adversaries against states' autonomy and influence.

Accordingly, the pursuit of control over the tech and digital sectors has been pushed by world governments through calls for sovereignty in digital spaces or, as the term evolved, through calls for digital sovereignty. The term corresponds to the classical definition of sovereignty: the state authority should be the supreme authority within one territory and for its citizens, thus trying to transfer such authority to digital spaces where the previously mentioned actors dominate. Although the claims towards digital sovereignty are being increasingly used, the term is surrounded by a sense of confusion since a clear definition doesn't exist. Moreover, various stakeholders often use the term in very different ways where meanings span across economic dimensions, protection of domestic industries to national security considerations.

The thesis aims to dig deeper into producing such claims by leaning on the existing constructivist literature and the social process through which different meanings of digital sovereignty are elaborated by different actors and how they interact with different political contexts and considerations (Santaniello, 2024). To do so, this thesis will focus on the EU and India and their relations with a focus on the digital dimension and their usage of the digital sovereignty concept.

The EU and India were selected because of the similarity of their position in the international system and current foreign policy goals related to the tech and digital sectors. Both entities are located in between the big geopolitical game between the US and China, trying to develop their digital strategies and be as independent as possible.

On one hand, the EU is looking to decrease its exposure to critical dependencies while improving its strategic autonomy (Kranenburg & Okano-Heijmans, 2023b, p. 5). On the other hand, India is looking to develop its high-tech sector and open up for more outside investments and cooperation (Ibidem, 6). At the same time, both the EU and India are

concerned with power distribution in the digital world and democratic values (Kranenburg & Okano-Heijmans, 2023a, p. 50).

Despite having a complex set of relations, the EU and India have grown to see their relations evolving into strategic cooperation. Recently, the EU and India have established the Trade and Technology Council (TTC) to ensure ”their technological and industrial leadership while preserving their shared values “ (Delivorias, 2024). TTC has been labeled as the strategic cooperation mechanism aimed at solving challenges “at the nexus of trade, trusted technology, and security” (*EU-India Joint Press Statement*, 2022). TTC with India is only the second such body established by the EU as the first one was established with the US in 2021.

The newly-created TTC between the EU and India added a new dimension to the existing relations. The essential goal of the TTC is to reach strategic autonomy through cooperation with a focus on digital governance, critical technologies, trade, and investments (Cogo Morales & Jorge Ricart, 2023). Moreover, one of the three working groups established within the TTC focuses on strategic technologies, digital governance, and digital connectivity (Delivorias, 2024). Although both the EU and India have similar values in their support for democracy and rule-based technology governance, the methodology both of them see as necessary differs significantly.

The approach both of them see as proper to pursue is thus essential for deepening their relations but both of them have goals to reach strategic autonomy and be more sovereign in the digital space. As both of them have diverging views on essential technologies such as Artificial Intelligence (AI), data governance, and 5G and 6G networks to name a few, differences in understanding of sovereignty in digital spaces can affect the relationship between each other.

After its inauguration in 2022, TTC became the main arena where such differences will be discussed and where the positions on these topics will be exchanged. Therefore, TTC can affect the previously discussed social process of elaborating digital sovereignty claims and affect the differences between the EU and India in the digital sovereignty domain. At the same time, TTC serves as the potential area for exchange of ideas on digital and critical technologies regulation.

Accordingly, this thesis aims to include the TTC in the analysis and respond to two following research questions:

1. How do the EU and India conceptualize and operationalize digital sovereignty, and what are the defining attributes of their sovereignty claims?

2. To what extent does the EU-India Trade and Technology Council (TTC) serve as a platform for addressing and potentially harmonizing the differing digital sovereignty discourses between the EU and India, and through what mechanisms, if any, might it contribute to such harmonization?

To respond to the questions a constructivist approach will be used with a focus on political discourse analysis (PDA). The PDA is an approach centered around the linguistic turn in political sciences concerned with the role of discourse in producing and maintaining power relations (Dunmire, 2012, p. 736). Driven by the perceived loss of control in digital spaces, the world's states increasingly use speech acts and discourse to reassert their power and authority (Werner & De Wilde, 2001). Moreover, national governments deploy these discourses in the field of digital technologies and ICT to further strengthen their sovereign powers (Budnitsky, 2022).

Accordingly, this thesis aims to delve into the process of producing power relations in digital spaces by observing how the idea of digital sovereignty has been used and operationalized in the official documents, policy strategies, statements, and legislations of the EU and India. The ex-post qualitative method will be used to discover the conceptualization of digital sovereignty by the EU and India. To accomplish so, this thesis (a) elaborates on the analytical framework to study the sovereignty claims using the body of literature using a constructivist approach to analyze digital sovereignty, (b) employs this framework to analyze the official documents of the EU and India, and (c) analyzes the capabilities of the TTC to address and harmonize the differences found in the previous step.

This study builds upon this literature by assessing the attributes of digital sovereignty claims by introducing more than one actor in analysis and studying the differences among them. Secondly, the current literature is predominantly focused on analyzing the claims for digital sovereignty of the EU neglecting the importance of other important

actors, namely countries coming from the Global South, such as India, Brazil, South Africa, and others that have developed their versions of the concept of digital sovereignty. Thirdly, with the EU-India TTC being officially launched in 2023, this study represents the addition to the literature that assesses the usefulness and capabilities of this newly established body providing policy implications. Finally, this study builds upon the literature that studies the current geopolitical dynamics and how actors other than the US and China can establish and strengthen their positions.

This study will be divided into the following chapters to respond to the research question presented. The first chapter will start from a broader perspective and scholarly work on how ideas, values, frames, and discourses shape international relations will be assessed. Putting classic sovereignty and its digital version into this framework, the goal of this review is to develop an analytical framework through which research questions will be answered.

The second chapter will focus on the existing relations between the EU and India positioning them inside the broader geopolitical context including digital developments and challenges. Moreover, the key documents that are dealing with their strategies in digital will be introduced.

The third chapter will focus on the empirical analysis of the documents based on the analytical framework previously developed. Here, the digital sovereignty claims of both the EU and India will be assessed and compared. Based on the similarities and differences found, the fourth chapter will assess the capacity of TTC to address them and give response to the second research question. The thesis will end with concluding remarks, some open questions for future research and policy implications.

2. Constructing Statehood in the Cyber Age

The end of the Cold War in the early 1990s brought an analytical gap in the IR studies as the prevailing realist and liberal school of thinking failed to explain the new dynamics within the International system. Although started before the 1990s, the constructivist theory gained significant traction in this period. Constructivism theory argues that actors shape the reality in which they operate, often through a mix of deliberate and unconscious processes. In international politics, this suggests that actors may be influencing their environment to align with their needs, whether intentionally or not. For instance, states' efforts to assert sovereignty in digital spaces could be seen as a response to perceived threats to their authority, though this construction may not always be a calculated strategy which is completely opposite of realist thinking that understands each state's action as the rational calculation.

The main goal of this chapter is to conduct a comprehensive literature review that maps out existing scholarly work on state sovereignty in digital spaces. This review aims to identify core concepts, recurrent themes, and diverse approaches and perspectives in the field. Additionally, it seeks to uncover gaps in current research. By synthesizing this information, the chapter will inform the development of an analytical framework that will be employed in subsequent chapters to examine how states construct their sovereignty in digital realms. Moreover, digital sovereignty and related concepts have widespread use, yet with different meanings and by different actors. Thus, it is necessary to identify the social process through which different meanings of digital sovereignty are elaborated by different actors (Santaniello, 2024).

2.1. How norms, ideas, and discourse shape international politics

During the Cold War years, the dominant understanding of the International system was centered around states and their power (Ejdus, 2017, p. 83). Moreover, the central debate was held between the realist and liberal school of thought about the possibilities of cooperation and challenges within the international system (Ibidem, 83). However, the swift end of the Cold War left many questions unanswered calling for different

thinking about the international system. Both realists and liberals couldn't answer a series of new developments.

From the realist perspective, theory struggled to explain the emerging unipolar world dominated by the US after the collapse of the Soviet Union. Realist theory predicted the power balancing against a hegemon. Moreover, realist thinkers argued that the key actors in the international system are states while the non-state actors were excluded as relevant. Yet, the rise of the non-state actors in the Post-Cold war period starting with the EU couldn't be explained with the sole focus on states. Finally, the increasing economic and cultural interconnectedness in the Post-Cold war period emphasized cooperation and interdependence contrary to realist notion of conflict.

On the other hand, liberal theory did predict correctly the increased importance of international institutions and economic interdependence but some questions remained unanswered. In the first place, the increased cooperation didn't underpin the peaceful world order as the conflicts emerged in the Gulf, Rwanda, and the Balkans. Secondly, globalization wasn't spreading at even speed and at everyone's benefit as predicted. On the contrary, the Post-Cold war period saw significant disparities between the Global North and South. Finally, the liberal theory couldn't explain the democratic backsliding that emerged with the rising authoritarian regimes. As proposed by Francis Fukuyama, liberalism anticipated the 'end of history' with global democratization.

The increased frequency of usage of digital sovereignty and similar concepts by actors globally without a clear definition opens the question of the nature of sovereignty. Realist theories suggest that sovereignty needs to correspond to a situation existing materially (Werner & De Wilde, 2001, p. 284). However, the increased usage of sovereignty by actors that materially are not sovereign (Martin, 2022, pp. 229–230) highlights the importance of the social process through which digital sovereignty and similar concepts are evoked.

Constructivist theory developed a framework over time to explain such a social process by analyzing some of the previously neglected aspects of international relations theory. The main contribution of constructivist theory to IR is the role of intersubjective knowledge and how ideas have constitutive effects on social reality (Adler, 2013, p.

123). The consequence of the intersubjective notion of reality that constructivism brings is that reality is collective so the facts in international politics depend on how states understand and comprehend them (Ibidem).

One of the seminal articles in constructivist thinking by Alexander Wendt argues the international system is what states make of it (Wendt, 1992, pp. 396–397). The core of the constructivist argument is that reality cannot be explained only in material terms.

On the contrary, how states perceive and express their positions is equally important, stating that reality is socially constructed. Wendt's example in the article mentioned previously states, “If the United States and the Soviet Union decide they are no longer enemies, ‘the Cold War is over’” (Ibidem, 397).

Consequently, the constructivist theory in IR studies tried to understand how factors outside the material world like discourse, language, and norms affected the dynamics of the international system. Some of the most important contributions of the constructivist theory are presented below.

The first contribution regards the understanding of change in the policy process. Constructivist theories add value by locating the origins of changes and social processes outside of material things. Moreover, constructivists locate the origins of change in the emergence of new rules, the evolution of social structures, and agent-related origins of change (Adler, 2013, p. 123). In other words, constructivist theory analyzes how actors influence and shape changes in international politics by advocating for certain ideas (Ibidem, 124).

They added previously neglected factors such as shared experiences, identities, ideas, and roles within certain institutions that can be summed under the term *logic of appropriateness*. This logic states that actors will adopt the solution to a certain policy problem not based on rational calculus, as rational theories understood, but based on the expectations of others inside a certain setting (Saurugger, 2013, p. 892).

Closely related to the understanding of change, the next two concepts that constructivist theory brought are *the understanding of the role of language* and *the understanding of discourse* which are heavily interrelated. In constructivist theory, language is seen as the

main vehicle for the diffusion and institutionalization of ideas (Ibidem, 125). In addition, constructivists argue that language is not only a tool that describes reality, but it is also a tool that constructs it (Ibidem, 125).

Following the role of language, *discourse* is another essential idea discussed by constructivist theory. Combining language and discourse, actors in international politics advocate for understanding a problem in a certain way that limits the range of alternative policy options (Adler, 2013, p. 125). One of the prime examples regarding the use of language and discourse in international politics is related to climate change issues. Oxley found that framing climate change issues as local rather than global problems and stressing the negative consequences can increase the voters' salience towards the issue (Oxley, 2020).

Constructivist theory also addressed the issue of perception that realist theories didn't manage to explain. Constructivists showed that the perception and pictures that actors in international politics have of each other are equally important as the actual, material state that exists (Herrmann, 2013, p. 5).

These perceptions can be powerful, generating a picture of other actors that is almost impossible to change. The classic example is the picture of the Soviet Union developed in the United States after the image created by John Foster Dulles (Ibidem, 11).

The final significant contribution of constructivist theory is the *understanding of norms* in international politics. The core idea of international norms, their definition, and their current existence in politics is not the focus of this study but the actual *process* through which international norms emerge and change. Two dynamics inside the norm-generating process are highly relevant to this study. First is norm vagueness as states are more likely to adopt vague norms so they can stick to their interpretation later (Van Kersbergen & Verbeek, 2007, p. 221). The more the norm is vague the more likely the clash for its meaning will occur later (Ibidem, 222). Secondly, the norm-generating process is not linear. On the contrary, norms are developed inside the communication process between the sender and receivers (Payne, 2001, p. 42).

2.2. Speech Act Theory

As part of a constructivist strand of IR research, the speech act theory emerged as a response to the dominating rationalist school of thought of IR embodied in the Realist school of IR. Yet, rationalist theories failed to answer certain questions that constructivism and speech act theories declared as crucial. One of them relates to how actors construct their identities and see themselves as agents (He, 2022, p. 77).

Because of the importance of language for this stream of thought, this turn in the IR studies was named the 'linguistic turn' (Ibidem, 77). However, the linguistic turn was only one of the many names used to describe the general reorientation of IR studies from positivism to reflexivism (Heiskanen & Beaumont, 2024, p. 9). The speech act theory is based on the presumption of the constructivist theory that words and language in general are not just tools that describe reality but also construct it. In other words, language precedes the world it forms (He, 2022, p. 80).

This new strand of thinking brought a division of reality into the material, the narrator and the receiver. Moreover, narrators are seen as actors who will make choices according to their conditions and purposes and spread their narrative texts trying to influence the recipients (Ibidem, 78). According to Gammeltoft-Hansen and Adler-Nissen, the current international system is witnessing "sovereignty games" in which states, as actors, are using speech acts as *moves* in these games to claim their authority and power (Gammeltoft-Hansen & Adler-Nissen, 2008, pp. 3, 8).

In closely related security studies, the turn toward reflexivity and language had an important influence as well. In security studies, securitization theory emerged because of a linguistic turn (Buzan et al., 1998). The securitization theory's main argument is that security issues do not necessarily reflect the material world but are more often a result of efforts of leaders and countries to understand and shape the world differently (Balzacq et al., 2016, p. 495).

On the contrary, any public issue can be pushed from being non politicized to politicized, meaning that a threat has been identified so emergency measures are necessary (Buzan et al., 1998, pp. 23–24). The move that a certain actor follows to frame the issue and move it from the established rules of the game is the securitization

move (Ibidem, 23). In other words, states are not only agents that are trying to construct reality using language, but they are also securitizing that same reality.

2.3. Sovereignty

The notion of sovereignty is one of the most complicated ones because it has its roots in multiple disciplines such as history, political science, law, etc. Not only does the term have roots in multiple disciplines, but it also underwent numerous changes throughout various historical periods.

From ancient Rome through the Peace of Westphalia and up to the 21st century, states in different formations have been trying to establish and confirm their authorities. Though different notions were used for such purposes, the notion of sovereignty emerged as the leading one defining states' authority. The origin of sovereignty stems from the words *supers* which means above in Latin and *so(u)verain* which means supremacy in Early French (Williams et al., 2012, p. 96).

As different challenges to states' authorities started to emerge, states were more eager to use and call for their sovereignty to be respected. The origins of sovereignty go back to Ancient Greece and Rome where the main question was whether the sovereignty was in the population or the ruler's body. This division continued up to Medieval times when the competition between the Church and a growing array of monarchs and secular rulers was present along with the Holy Roman Empire. The results of such competition resulted in the "Christian unity under God" that was also known as the *República Christiana* or Christendom (Ibidem, 99).

The notion of *respubilca* was further developed in the writings of Machiavelli, Hobbes, and most importantly, Jean Bodin. The result was the political unit or polity with the definition of sovereignty being "the supreme authority within a given territory" (Ibidem, 101). The Thirty Years' War (1618-1648) that followed resulted in three peace treaties: one concluded at Osnabrück and two at Münster which are collectively known as the Peace of Westphalia.

The Peace of Westphalia was arguably the most important event in the development of the contemporary concept of sovereignty because of two consequences it brought:

- The emergence of the sovereign state as the singular mode of European authority and vesting the authority within the state and not the body of the ruler
- The promotion of legal equality which states that sovereign states must recognize the rights of other states to claim the same (Ibidem, 104)

The notion of sovereignty that emerged from the Peace was marked as Westphalian sovereignty (Krasner, 1999, pp. 3–14). Every state is made of territory, people, and government (James, 1999, p. 460). In contrast, a polity is confined by borders inside which a state has supreme authority (Williams et al., 2012, p. 101). Sovereignty has its internal and external dimensions. Internally, sovereignty represents the governing authority over everybody who lives inside its territory while externally, the state is equal to other states and needs to be respected accordingly (Jackson, 1999, p. 433).

The mentioned notion of sovereignty was further consolidated and redefined. The most important redefinition included the emergence of colonialism in world politics when different understandings were to be created for nationalities of "non-Western cultural system". More precisely, the connection between sovereignty and the specific set of cultural values was developed at the exclusion of others (Anghie, 1999: 5 as cited in Williams et al., 2012)

2.3.1. Westphalian Sovereignty Decline

As the notion of sovereignty was evolving, so did challenges to it that put some of the dimensions of the term on the test. All these challenges can be summed up under the name of globalization that, according to Gammeltoft-Hansen and Adler-Nissen, can be divided into four specific dynamics (Gammeltoft-Hansen & Adler-Nissen, 2008, pp. 4–5):

- The development of international cooperation and international institutions. States delegated many of their sovereign functions to international organizations whereas this process went the furthest in the case of the EU.

- The increased amount of flow of people, commodities, and capital across borders makes it hard for any sovereign states to manage them.
- The process of decolonization is where numerous states are struggling to exert authority inside their borders.
- The evolution of international law that limits states' capacities to exert their power as a supreme legal authority

The four previous dynamics showcase that the scope of activities over which states can exert control is declining (Krasner, 1999, p. 12). Westphalian sovereignty previously mentioned and understood as a supreme authority within a certain territory is challenged as numerous outside actors have different parts of states' authorities and jurisdiction. Threats to sovereignty emerging from globalization created a whole strand in political science literature that declared sovereignty as an obsolete term that no longer exists as states cannot exert it.

The rationales behind the erosion of sovereignty, as explored in these studies, can be situated around two sets of arguments. The first strand takes the global policy perspective and argues that because of the nature of policy problems that are going beyond nation-states, international institutions are gaining more significance and thus, lowering states' capacities to exert their sovereignty (Soroos, 1986, pp. 6, 14).

This strand focuses on the different aspects of sovereignty that are no longer in states' hands because of the nature of the problems facing. The economic sovereignty of countries has been given to organizations such as the World Trade Organization (WTO) and the World Bank. Political sovereignty, on the other hand, has been handed out to organizations such as the OECD and the EU (Gammeltoft-Hansen & Adler-Nissen, 2008, p. 4). The common trait of these organizations is that they are public.

The second emphasizes the international economy and capital movements pressuring nation-states and lowering their control (Stiglitz, 2006, p. 21). Moreover, the global economy is run by a transnational elite that is controlled by transnational capital pursuing the goal of decreasing states' capacities to govern their economies and societies (Robinson, 1996, p. 4). The term used for these companies is multinational

companies that control resources most world countries need to tackle their challenges. Moreover, it is not just that these companies can solve government problems, but they are often responding to public demands (Terzi & Marcuzzi, 2019).

Furthermore, the internet being one of the key elements of globalization increasing global connections between countries, people, and economies influenced the development of types of sovereignty that didn't exist before such as digital sovereignty, data sovereignty, technological sovereignty, etc. Moreover, the increased interconnectedness made available by the internet and globalization reshaped Westphalian sovereignty creating what Krasner calls interdependence sovereignty (Krasner, 1999, p. 4). This sovereignty marks the state's capacity to regulate the flow of people, goods, and information across its borders (Ibidem, 5).

2.3.2. Constructivist Rethinking of Sovereignty

Once the world states started evoking their sovereignty more frequently while, materially, losing it, the constructivists' understanding of international politics became actual again. Contributions of constructivism previously discussed can be applied to sovereignty. Constructivists argue that sovereignty is a social construction developed, defined, and refined by states through their speech acts (Thomas J., 2013, p. 252). Following the constructivist logic, states may try to express their sovereign claims that don't match their actual sovereignty. Furthermore, other states may not express sovereign claims at all but are sovereign, nevertheless.

Ultimately, the implication of undertaking a constructivist approach towards sovereignty is the distance between material and reality that states constructed. The constructivist theory argues that sovereignty should be understood as a speech act, as a claim to authority rather than an institutional fact (Walker, 2006: 6–7 as cited in (Gammeltoft-Hansen & Adler-Nissen, 2008, p. 6). As Santaniello argues, to fully understand the notion of sovereignty, it is necessary to investigate the attributes of its claims to it (Santaniello, 2024).

States are using the power of language and discourse to construct a reality in which they perceive themselves as sovereign actors. More precisely, they conflict their claims with

the claims of other states in what Gammeltoft-Hansen and Adler-Nissen call the sovereignty games (Gammeltoft-Hansen & Adler-Nissen, 2008). In these games, states are deliberately trying to generate (construct) the reality in which they are perceived as sovereign and thus, reach their policy goals (Ibidem, 5). Furthermore, states are using these claims to create a separation between outside and inside (Adler, 2013, p. 127).

These claims are more likely to be evoked during the time the states' sovereignty is threatened to be diminished (Werner & De Wilde, 2001, p. 284). Because of that, the claims to sovereignty are at the same time securitization acts that focus on certain threats to their sovereignty justifying, at the same time, extraordinary measures to tackle them.

Due to the increased power of numerous actors within the digital field and the internet, the ongoing trend is more frequent use of sovereignty claims in the digital field that caused the emergence of sovereignty modifications such as digital sovereignty, data sovereignty, internet sovereignty, etc. Inside of these claims, big companies, organizations, and different activities have been marked as the main threat.

The constructivist rethinking of sovereignty carries significant implications for both traditional and digital sovereignty. This approach views sovereignty as a social construction shaped by states' speech acts rather than material realities, revealing a potential gap between sovereign claims and actual authority. States engage in "sovereignty games," using discourse to construct themselves as sovereign actors, especially when they perceive their authority as threatened. These claims often function as securitization acts. In the digital realm, this perspective has led to new sovereignty modifications such as digital, data, internet, and other digital variations of sovereignty.

2.3.3. Digital Sovereignty

So far, it has been discussed about the origins of sovereignty, the development of modern, Westphalian sovereignty, and its decline due to the different forces of globalization and the theoretical rethinking that a constructivist theory brought. As will be shown later, the focus on Western tradition in sovereignty research has been transferred into the contemporary political thought and analysis of digital sovereignty.

All these dynamics transferred into the digital world causing the states to seek their sovereignty in digital spaces. The process of digitization that started in the 1990s with the development of the worldwide web initiated a significant macro social transformation through two related trends: the spread of connections in digital space and the increased amount of digital data collected and cross-border data flows (Pohle, 2020, p. 6). These trends marked the essential change in which modern economies and societies work.

Digital spaces and the internet account for a significant part of the production of modern economies as they allow e-commerce transactions, share digital media content, and possess digital enabling infrastructure (Reinsch et al., 2020, p. 18). Moreover, the usage of the internet in modern economies has positive spillover effects in the form of free digital goods available to users (Ibidem, 19) such as email providers, search engines, communication applications, etc. These tools are based on the collection and processing of a huge amount of data that further enhances the effectiveness of digital economies (Popkova, 2023, pp. 3–4). Data that has been collected through the functioning of the digital economy has to be stored in clouds giving additional importance to data storage and the location of these clouds (Ibidem, 6).

The economic data shows that the internet has had a positive and significant impact on economic growth (Choi & Yi, 2009) while at the same time creating challenges for world countries and policymakers. The biggest three challenges relate to the market power of companies and actors controlling the internet, the dependencies of governments on them, and the borderless structure of the internet.

- **Market Power**

Due to the control of digital spaces by a handful of actors, there has been an increased trend of concentrating market power globally. Digital spaces and the internet are run by capitalistic and technological elites looking to maximize benefits and profit margins (Gu, 2023, p. 4). These actors dominate computing power, data itself, and algorithms used for their analysis while constantly expanding their operations worldwide and in different spheres of economies (Ibidem, 8). As the market power of these companies grows, the long-term effect on economies is the discouragement of innovation and entry

barriers for non-superstar firms along with the reduction of productivity (Aghion et al., 2021, p. 8).

The main actors in this regard are the biggest world companies that operate telecommunication systems, search engines, hardware, and cloud services. These companies are often known under the acronym GAFAM (Google, Amazon, Facebook, Apple, and Microsoft) representing the biggest US companies. Recently, the acronym of BATX became popular as well, marking the biggest Chinese companies in the digital field: Baidu, Alibaba, Tencent, and Xiaomi (Nicole, 2024).

Besides the biggest companies, startups emerging worldwide are also emerging as a challenge to states because of their influence in some of the most important technologies. These startups are emerging in fields such as AI and Data Science, advanced computing, Blockchain and Decentralized systems, etc. (*30+ Top Tech Startups & Companies in 2024: Shaping the Future*, 2024).

➢ **Governments' dependence on digital spaces**

Not only that the market power of companies and other actors grew significantly but, at the same time, governments became increasingly dependent on their services and business models. These actors are in control of data, research and development, industrial value chains, and data generation thus affecting and making modern economies depend on them (Gu, 2023, p. 11). The ongoing processes of data collection, AI development, and machine learning are being increasingly perceived as the most important arena for state competition and power struggles. Thus, the states are becoming increasingly dependent on them to gain a geostrategic advantage (Christakis, 2020, p. 42).

The COVID-19 pandemic exposed the dependence of governments on companies regulating the internet as people's lives were moved to online spaces due to the pandemic allowing these companies to gather even bigger power due to the collection of personal data (Ibidem, 11). In addition, it should be noted that these two processes enforce each other. As the importance of data grows over time, more governments become dependent on these actors. As reliance on companies grows, the more their market power grows (Ibidem, 2).

Numerous authors like Nick Couldry and Ulises Mejias viewed this growth of data's importance as a sort of introduction to a new colonial relation called data colonialism (Couldry & Mejias, 2019). The authors include Big Tech corporations, startups, and other software companies in what they call the *social quantification sector* (Ibidem, 340). Actors within this sector are capturing the everyday behavior of people in the world, translating it into quantitative data that is later used for profits (Ibidem, 340).

➢ **The Borderless Structure of the Internet**

Since the introduction of the internet, it was clear that its structure was without a central authority. The Internet Governance Project labeled globality as being one of the key characteristics of the Internet (Mathiason et al., 2004, p. 7). The project went on to describe the Internet where established communication is non-territorial and that "routing structure is insensitive to distance and political boundaries" (Ibidem, 7). Not only that the structure of the internet is borderless, but at the same time it is also fluid and subject to constant changes in its operation (Gu, 2023, p. 4) (Mathiason et al., 2004, p. 5).

Not only is the internet borderless thus lowering the states' capacities to regulate it, but it is also under the domination of non-state actors. Because of the nature of the Internet, the term *governance* has been used instead of the term *government* because it requires coordination among numerous actors including, besides governments, civil society, business, academia, developers, network operators, etc. (Internet Governance Forum) (Glen, 2014, p. 642).

From the earliest phases of the internet, inside this governance system, non-state actors have played prominent roles (Ibidem, p. 641). Besides already mentioned actors, the most notable roles have been held by the Internet Corporation for Assigned Names and Numbers (ICANN) which operates as a private, nonprofit organization governed by California law and that allocates the internet's domain names and IP addresses (Ibidem, 641).

Other institutions that participate in Internet governance and that represent the challenges for states' authorities are the Internet Governance Forum (IGF), International Telecommunication Union (ITU), etc.

Occasionally, these actors gather in conferences and meetings to discuss important issues regarding the Internet. Some of the most important ones were the two UN-sponsored World Summits on the Information Society (WSIS) that were held in Geneva in 2003 and Tunis in 2005 (Ibidem, 642) and the World Conference on International Communications (WCIT) held in Dubai in 2012.

2.3.4. The Development of Alternative Discourses

The rise of market power, the borderless structure of the internet, and the dependencies of states towards digital spaces mark the challenges states are currently facing in digital spaces. However, as Floridi argues, the most visible clash is the one between companies and states (Floridi, 2021, p. 3). These challenges caused a significant increase in the frequency of using the term digital sovereignty. The study by Couture and Topin discovered that the frequency of the use of the notion of sovereignty related to digital has grown significantly when the period before 2011 and the period from 2015 to 2018 are compared (Couture & Toupin, 2019, p. 2306) (See Table 2.1).

Table 2.1 - Digital Sovereignty and similar terms frequency of usage

	Data Sovereignty		**Technological Sovereignty**		**Digital Sovereignty**	
	Academic	**Other**	**Academic**	**Other**	**Academic**	**Other**
Before 2011	0	23	12	81	0	6
2011-2014	18	794	6	101	2	49
2014-2018	89	2459	20	131	22	239

Note. Reprinted from: Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305–2322.

Before 2011, one of the first mentionings of sovereignty in digital spaces was in 1996, in the Declaration of Independence of Cyberspace where the author, John Perry Barlow, asks governments of the industrial world to stay out of cyberspace saying: "You have no sovereignty where we gather." (Barlow, 1996).

The internet and digital space started to grow mostly under the dominance of the US private sector with the absence of any rules regarding the management of the new system (Martin, 2022, pp. 227–228). The first calls for digital sovereignty came from China and Russia who felt the most vulnerable due to American dominance (Ibidem, 228).

China was the first to call for digital sovereignty, framing its claims as cyber sovereignty or internet sovereignty (Pohle & Thiel, 2020, p. 8). The primary focus of these claims was the non-intervention of Western social media and information from entering the space under Chinese jurisdiction (Broeders et al., 2019, p. 2).

Similar events happened in Russia as the country tried to block access to unapproved content entering its cyberspace (Jansen et al., 2023, p. 1). At the same time, Western countries denounced these attempts as a Trojan horse for the introduction of more strict government controls favoring free information flows and open internet (Ibidem, 1). The main fears of the Chinese and Russian governments were the protests and Arab Spring that happened in 2011 along with the essential role of social media in them (Broeders et al., 2019, p. 2).

The differences related to the management of digital spaces were shown during the 12-day WCIT conference in December 2012. The clash was between the open multistakeholder model supported by the US and its allies that advocated for a status quo and decentralized, free market approach (Glen, 2014, p. 645). On the contrary, the proposal known as Contribution 27 was advocated by Russia, China, Saudi Arabia, and others challenging the existing Internet governance framework calling for more national controls and shifting the responsibilities to multilateral government bodies, such as the ITU (Ibidem, 647).

The most important event happened on June 5, 2013, when the technical specialist in the US National Security Agency (NSA), Edward Snowden, revealed that the NSA was monitoring more than 35 world leaders and intercepting communications from more than 50,000 computer systems worldwide (Chander & Le, 2015).

Snowden revelations marked a significant turning point not just because of the increased usage of digital sovereignty and similar terms but also because of the shift

expressed by the Western governments, particularly the EU countries. The narrative turned from support to free information and data flows to claims for more sovereignty (Couture & Toupin, 2019).

Current claims for digital sovereignty can be understood from three perspectives (Pohle & Thiel, 2020, pp. 8–13):

1. State autonomy and security focus on the geographical restriction of sovereignty to a certain authority within a certain territory and states' efforts to protect their data and digital infrastructure from foreign surveillance.

2. Economic autonomy and competition focus on domestic economies and their abilities to innovate and compete making national economies autonomous from foreign technologies and service providers.

3. User autonomy focuses on the protection of citizens as employees, consumers, and users of digital technologies and services.

Besides these three, other authors also discovered digital sovereignty claims aimed at protecting indigenous groups and social movements (Couture & Toupin, 2019).

Digital sovereignty claims have many permutations that follow previous divisions depending on the point of view being state, economy, or individual. The first one of them is cyber sovereignty used mostly by China and Russia in a way that foreign intervention is seen as a threat to their political systems. These claims see their sovereign cyberspaces threatened by Western service providers and big companies (Jansen et al., 2023) trying to develop their alternatives such as Great Firewall in the case of China (Martin, 2022) or 'RuNet" standing for Russian Internet in the case of Russia (Ibidem). Besides cyberspace sovereignty, these actors also tend to use the term internet sovereignty (Pohle & Thiel, 2020, p. 8).

The EU approach towards digital sovereignty tends to be the most complicated one because it combines state, economy, and personal perspectives while using different terms. The term technological sovereignty has been used in a way to protect the EU economy and keep it competitive by being independent in terms of vital minerals, technologies, and digital supply chains, for example, in the semiconductor industry

(Jansen et al., 2023). At the same time, these aspirations of the EU also have broad geopolitical implications in positioning itself in a broader Sino-American geopolitical battle. That's why the term strategic autonomy is often being used (Ibidem, 3) (Christakis, 2020).

Ultimately, the term data sovereignty is used also as data localization (Jansen et al., 2023) or data nationalism (Chander & Le, 2015). Data is the vital aspect of sovereignty, so it represents the wide term that includes all the previous ones because without data there is no digital, internet, or technology sovereignty (Jansen et al., 2023). Except for data, sovereignty is often used with some crucial technologies such as AI sovereignty or *5G sovereignty* (Floridi, 2021, p. 8).

Claims for authority over the Internet through digital sovereignty and similar concepts have spread worldwide recently and not just in countries that were mentioned before. The study by Chander and Le included a sample of 16 countries from all the continents finding out that each wanted to exert certain control over the internet because of concerns over privacy, security, surveillance, etc. (Chander & Le, 2015).

2.4. Digital Sovereignty in the EU - Overview

In the final part of this chapter, the body of literature using a constructivist approach to analyze digital sovereignty claims was assessed. During the assessment of contemporary research on digital sovereignty, several research gaps were identified. In the first place, as the debate on classical sovereignty, the research of digital sovereignty has predominantly found ground in the Western tradition of sovereignty. The dominance of the Western tradition carries onto the contemporary constructivist literature on digital sovereignty as the majority of studies are focused solely on the EU and the US while leaving the majority of countries, such as India, outside of the analysis.

Secondly, a body of research focused solely on one actor and used analytical frameworks made for a single-actor analysis. Finally, none of the research focused on the capacity of certain bodies or institutions to bridge the gap between differences in digital sovereignty understanding among various actors.

Accordingly, the studies analyzed and their analytical frameworks are based on the two following approaches:

1. Discourse analysis of policy documents and strategies
2. Theoretical analysis of the notion of Digital sovereignty and similar concepts

In the sections ahead, both of these approaches and frameworks used will be analyzed as the ground for developing a new, adjusted analytical framework applicable to the research questions mentioned above and able to bridge the research gap identified.

2.4.1. Discourse Analysis Approach

The discursive analysis understands sovereignty as a speech act, as a claim made to justify a certain actor's exercise of power (Werner & De Wilde, 2001). This strand of digital sovereignty analysis is the most frequent one with various methodologies applied across multiple sectors such as healthcare (Pierri & Herlo, 2021), finance (Donnelly et al., 2024), or internet regulation in the EU (Perarnaud & Rossi, 2024). Other strands, while preserving the same methodology, were more focused on specific countries such as France, Germany (Dammann & Glasze, 2023), and India (Kumar & Thussu, 2023). Ultimately, some research articles covering digital sovereignty focused on how efforts pursuing digital sovereignty were to form and create national identities (Budnitsky, 2022). This strand is particularly important because it sees governments as actors that deploy digital technologies as support for building their national identity. (Ibidem,)

While the research papers presented above are valuable for gaining more insights into the notion of digital sovereignty, the essential ones for this thesis are the ones that assessed the characteristics of claims containing digital sovereignty (Santaniello, 2024). More precisely, these articles focused on the interplay between a sovereignty claim made by certain actors and the existing power relations (Ibidem, p. 1920-1921). Accordingly,

The main analytical difference between these articles came from the purpose of the analysis. In general, this strand of literature can be divided into two analytical goals: **The relationship between discourse change and policy change (policy output)** and **the social process through which different actors construct their digital**

sovereignty. Articles were identified through research of academic databases[1] using keywords *digital sovereignty, technological sovereignty,* and *data sovereignty.*

The subsequent portion of this section will present selected analytical frameworks employed in the aforementioned papers, which will serve as the foundation for developing the analytical framework of this thesis. See Table 2.2 for more details.

Table 2.2. - List of Articles Analyzed

Author(s) & Year	**Title**	**Key Contribution to Framework**
André Barrinha & G. Christou. (2022).	Speaking sovereignty: the EU in the cyber domain	Establishment of criteria used to discover the meaning of digital sovereignty claims and the consequences of such claims.
Julia Carver. (2024).	More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy	Establishment of criteria used to analyze the significance of digital sovereignty discourse within textual material.
Gerda Falkner, Sebastian Heidebrecht, Anke Obendiek, and Timo Seid. (2024).	Digital sovereignty - Rhetoric and reality	Establishment of criteria used to analyze the significance of digital sovereignty discourse within textual material.
Daniel Mügge. (2024).	EU AI sovereignty: for whom, to what end, and to Whose benefit?	Establishment of contentious dimensions of digital sovereignty.
Mauro Santaniello. (2024).	Digital Sovereignty in the Euro-Mediterranean Region	Establishment of criteria used to uncover the meaning of digital sovereignty claims and understand the consequences of those claims within power dynamics.
Daniëlle Flonk, Markus Jachtenfuchs & Anke Obendiek. (2024).	Controlling Internet content in the EU: towards digital sovereignty	Definition of problems identified by digital sovereignty discourse and the prescriptions proposed by the actor making the claim.

Analysis done by Julia Carver uses the institutionalist approach to analyze how discursive change has driven policy change (Carver, 2024, p. 6). To do so, the paper stresses the importance of a particular institutional context and focuses on the explicit

[1] Following databases were used: Sage Journals, Taylor & Francis, and JStor.

use of digital sovereignty in the EU's external policies (Ibidem, 7). To capture the discursive change, explicitly mentioning the digital sovereignty term is analyzed through the following criteria: sequencing, significance, and distinctiveness (Ibidem, 7-8). More precisely, for the discursive change to be captured, the change must occur before the policy change.

Furthermore, the digital sovereignty concept is expected to solve the problems identified and apply them to the solutions. Finally, the discursive change resulting in the increased usage of the digital sovereignty term must be distinctive. In other words, the effect of the discursive change must be empirically distinguishable from other factors influencing the policy change (Ibidem, 7-8). Based on the presented criteria, the author was able to identify where a discursive change was significant and explain the relationship to policy change. The analysis performed by Julia Carver relies on previous research done by the group of authors (Falkner et al., 2022).

As the first paper by Julia Carver, the second analysis uses the same analytical framework, focusing on the exclusive references of digital sovereignty and similar terms such as tech sovereignty, cloud, or data sovereignty (Ibidem, 4). Accordingly, the second analysis also uses the criteria of relevance and applicability as the essential criteria for identifying significant discursive change (Ibidem, 4) (See Table 2.2).

Table 2.2 - Julia Carver Analytical Framework (Carver, 2024)

Level of Analysis	Criterion	Observed?	Relationship to policy change
European digital sovereignty discourse as a core set of ideas	Temporarily before policy change?	Yes	Plausible causal role (necessary, not sufficient)
		No	Doesn't drive policy change
	Significance?	Yes	Comprehensive
		No	Inconspicuous
	Distinctiveness?	Yes	Distinctive
ndividual 'European sovereignty' concepts in policy discourse		No	Indistinctive

Note. Reprinted from: Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy*, 1–37.

From a slightly different perspective, another paper by Flonk, Jachtenfuchs, and Obendiek used discourse analysis to assess the relationship between discourse and policy change (Flonk et al., 2024). The study aims to analyze the digital sovereignty discourse by looking at the content control of the EU.

To do so, the study develops the analytical framework divided into two dimensions: *policy discourse* and *policy output* (Ibidem, 3). To analyze policy discourse, the study uses two frames as the ideal types of discourse: *free access discourse* and *public order discourse* (Ibidem, 5). For more details, see Table 2.3.

Table 2.3. - Policy Discourse Frames

Frame	Problem Definition	Prescriptions
Free access	The restriction of free access to content is a threat to liberal democracy	Self-regulatory solutions, empowerment of individuals or specific groups, such as parents with limited state intervention
Public order	The public order and the public interest are under threat from internal and/or external forces	Comprehensive public regulatory interventions to strengthen public control

Note. Reprinted from: Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: Towards digital sovereignty. Journal of European Public Policy, 1–27.

For the analysis of the policy output segment, the study uses three criteria to do the assessment: *volume* which refers to the number of documents produced over time, *bindingness* understood as non-law, soft law, and hard law, and *orientation* which refers to the distribution of across different policy areas (Ibidem, 6).

The first study that will be presented here is the study by Daniel Mügge that deals with a specific aspect of digital sovereignty, AI sovereignty (Mügge, 2024).

The article analyses how the EU constructs and understands its sovereignty by asking three questions:

1. For whom is sovereignty to be won?
2. What is the objective of AI sovereignty?
3. What is the scope of its envisaged beneficiaries? (Ibidem, 2)

The three questions form three dimensions of AI sovereignty presented in the paper: subject of sovereignty (jurisdictional sovereignty, citizen sovereignty), objective of sovereignty (Boost competitiveness, Emancipate EU AI policy from competitive pressure), and scope of envisaged beneficiaries (Global, Euro-centric) (Ibidem, 3). To perform the analysis, the study analyzed seven documents that summarize the European Commission's (EC) AI strategy.

The aforementioned analytical frameworks are important because of common steps they use to reach their findings:

- ➢ All articles are using a structured approach in which the first step includes narrowing down the sample of documents analyzed using different criteria. They are used to identify whether a certain document or statement possesses a significant digital sovereignty discourse by establishing criteria of centrality, relevance, and applicability (Carver, 2024; Falkner et al., 2022).
- ➢ Based on previously developed dimensions, the articles track recurring themes, words, and narratives. They are used to identify frames through which the digital sovereignty discourse is described, the goals of the discourse, and the main adversaries (Flonk et al., 2024; Mügge, 2024).

2.4.2. Theoretical Approaches to Digital Sovereignty Analysis

Scholars who undertook a theoretical approach analyzed the claims different actors made about digital sovereignty to understand what the notion of sovereignty means in digital spaces (Couture & Toupin, 2019).

What all the studies taking theoretical approach have in common is the division into three dimensions, depending on the sector the notion of digital sovereignty is used in (Pohle, 2020; Pohle & Thiel, 2020) (Couture & Toupin, 2019): State autonomy and security, Economic autonomy and competition, and Individual dimension.

Theoretical approaches presented here are beneficial for the analysis of digital sovereignty because they can discover the motivation behind the discourse used in statements, policy documents, and other materials and summarize whether the position of the actors leans more towards state autonomy, economic autonomy, or individual dimension.

Besides these three contained in all the papers, other notions of digital sovereignty were identified with less frequency such as cyberspace security that sees digital spaces outside of state jurisdiction, digital sovereignty of social movements (Couture & Toupin, 2019), and indigenous digital sovereignty (Kwet, 2019; Pinto, 2018).

3. Research Design and Methodology

Research framework presented builds on the gap found in the literature and the findings from articles discussing digital sovereignty. In the first place, currently prevalent frameworks are used to analyze digital sovereignty of a single actor. On the contrary, the research framework pursued here will be applied to two actors. Secondly, the current body of literature analyzes recurring themes, words, and narratives inside of policy documents. Framework presented here enhances this by introducing a body that has a jurisdiction to interfere in the discourse creation and thus, affect and change the prevalent words, themes, and narratives. Finally, to adjust the framework to the specific case of the EU-India, the individual dimension of sovereignty that debates about individual sovereignty and human rights is left out of the analysis (Couture & Toupin, 2019).

As in the body of literature analyzed, this study pursues an *ex-post* qualitative method through which policy documents, statements, and official reports will be analyzed to find prevalent themes, words, and narratives. The process follows a structured, multi-step framework.

➢ **Step 1 - The Significance of Digital Sovereignty Discourse**

To assess and define how the EU and India operationalize digital sovereignty in their documents the first step is to analyze which documents contain digital sovereignty discourse that is significant. Such analysis will be performed through a qualitative analysis of the sample materials by looking at the explicit use of the discourse of digital sovereignty (Carver, 2024, p. 7). The criteria for the significance of digital sovereignty discourse are presented in the table below (See Table 3.1). In order for the document to be labelled as having a significant digital sovereignty discourse, the document needs to have all three criteria: centrality, relevance, and applicability fulfilled.

Table 3.1 - Filtering materials with significant digital sovereignty discourse

Criterion	Definition
Central	Materials contain problems/challenges related to the digital sphere and the term digital sovereignty and alternative concepts that have the highest frequency in them.
Relevant	Materials contain proposals that are expected to address problems/challenges identified and are feasible to solve.
Applicable	Materials specify strategies and steps on how digital sovereignty discourse should solve the problems/challenges identified.

Note. Criteria and definitions are elaborated from Carver's and Falkner's papers and adapted so as to respond to research questions addressed in the present work.

➢ **Step 2 - Thematic and Narrative Identification of the Discourse**

After the first step is performed, in the second step the sample will be reduced and documents with a significant portion of digital sovereignty sorted. The selected materials will then be filtered to another set of criteria used to analyze the type of digital sovereignty discourse used. The criteria are based on three questions. Each question entails two competing ideal-typical alternatives (Mügge, 2024, p. 2) around which any material is centered around. Moreover, each of the two alternatives within the question will be quantified as values 1 or 2. The full explanation is presented in the table below (See Table 2.5).

Table 3.2 - Analysis of Digital Sovereignty Discourse

Question 1	Who or what is seen as the problem?	
Answers	Digitalization	Tech Platforms/Big Tech
Value	1	2
Question 2	What is the goal of the Digital sovereignty discourse?	
Answers	Competitiveness	State Security
Value	1	2
Question 3	What are the means proposed as a solution?	
Answers	Standardization/Regulation	Protectionist Measures
Value	1	2

According to the criteria, each document will receive a value between 3 and 6 with values 3 and 4 being closer to the more economic version of digital sovereignty. On the other hand, values 5 and 6 represent more security-oriented discourse. The table below contains more details (See Table 2.6.).

Table 3.3 - Acquiring Results

Value	3,4	Economic DS	Creating an economic context that favors technological innovation within the national territory. Fostering autonomy of the national economy concerning foreign technology and service providers.
	5,6	Security DS	Emphasis is put on controlling digital infrastructure within national borders and tackling constant monitoring of citizens performed by foreign countries, namely the US.

Note. Criteria and definitions are partly taken from Couture and Topin's and Pohle and Tiels's papers and adjusted to the research question of the thesis.

By running sample materials with a significant portion of digital sovereignty discourse through the presented criteria, the analysis aims to obtain average numbers for the EU and India separately. The phase will conclude with the average numbers for both the EU and India. Thus, respond to the first research question related to conceptualization, operationalization, and defining attributes of digital sovereignty claims in the EU and India.

➢ **Step 3 -Introducing the TTC to the Digital Sovereignty Analysis**

The final step of the analytical framework involves a qualitative analysis of the three working groups that form the foundation of the EU-India Trade and Technology Council (TTC): 1) Strategic technologies, digital governance, and digital connectivity, 2) Green and clean energy technologies and 3) Resilient value chains, trade, and investment (Delivorias, 2024).

Building on the findings from the previous two steps, this phase identifies key technological areas covered by the TTC's work. These areas are selected based on their potential to either align (converge) or further separate (diverge) the EU and India's approaches. Ultimately, by examining the role of the working groups within the TTC, this analysis will assess the council's overall impact on these technological areas,

addressing the second research question and the ability of the council to act as a facilitator in digital sovereignty discourse relations.

Sample of Documents

The sample is made of 24 documents in total. Documents have been acquired by typing keywords such as *digital sovereignty*, *sovereignty*, *data sovereignty*, and *technological sovereignty* into search bars available on the EU Commission website and the website of the Indian Ministry of Electronics and Information Technology, the website of the Indian government. Documents are divided into three categories: key policy documents, policy statements of officials, and reports by official bodies (See Table 2.8).

Such division was followed because it allows this thesis to show how digital sovereignty and similar discourses are conceptualized and operationalized in long-term strategic documents and short-term statements by key officials. Officials are selected based on the offices they're in charge of (See Table 2.7). Finally, reports that track the current state issues related to digital sovereignty and related issues are selected because these provide context on implementation, specific initiatives, and governmental monitoring of digital sovereignty goals. Moreover, the specific documents were selected based on two criteria:

- Documents cover the area of expertise under jurisdiction of the TTC such as AI, Cybersecurity, strategy in digital spaces, etc.
- Each document from the side of the EU is matched with the document from the side of India ensuring the focus on comparable themes.

The selected documents cover the period from 2018 to the current moment. The selected time has been chosen for the following reasons that are according to the research question of this thesis. In the first place, Snowden revealed in 2013 that the NSA was intercepting communications and acquiring intelligence from leaders. Snowden revelations marked an important turning point as the governments, mostly the ones from the EU, became aware of problems related to digital sovereignty and the ability of the state to control communication platforms and services (Chander & Le, 2015). Up to 2018, the EU became fully aware of the issues related to digital sovereignty and

included the discourse in the program of the new European Commission inaugurated in 2019 (Von der Leyen, 2019).

Secondly, as world governments became more aware of the issues related to the digital world after 2018, the COVID-19 pandemic marked another turning point. The pandemic showed how much governments are dependent on digital technologies owned by private actors (Burgess, 2020; Christakis, 2020, p. 42). Ultimately, India banned Chinese-owned social media platform, TikTok, in 2020 following the clashes on the Sino-Indian border. The wave that started with TikTok ended with the ban of more than 50 apps from Chinese companies in India (Kumar & Thussu, 2023, p. 1584; Mehrotra, 2022).

Table 3.4 - The List of Key Officials

Name	**Office Held**	**Actor**
Ursula Von der Leyen	The European Commission President	EU
Margarethe Vestager	Executive Vice-President for a Europe Fit for the Digital Age	EU
Thierry Breton	Commissioner for Internal Market	EU
Narendra Modi	Prime Minister	India
Piyush Goyal	Minister of Commerce and Industry	India
Jitan Ram Manjhi	Minister of Micro, Small, and Medium Enterprises	India
Ashwini Vaishnaw	Minister of Electronics and Information Technology	India

Table 3.5 - The List of Key Policy Documents, Statements, and Reports

Type	EU	India
Key Policy Document	AI Act	National Strategy for Artificial Intelligence
Key Policy Document	European Commission digital strategy: Next Generation Digital Commission	Digital India
Key Policy Document	A European Strategy for Data	The Digital Personal Data Protection Bill
Key Policy Document	2030 Digital Compass: the European Way for the Digital Decade	Strategy for New India @ 75
Key Policy Document	The EU's Cybersecurity Strategy for Digital Decade	The National Digital Communications Policy
Statement	Commission approves €5 billion German State aid measure to support ESMC in setting up a semiconductor manufacturing facility.	India is emerging as a hub of global trade and manufacturing: PM Modi
Statement	Executive Vice-President-designate for Tech Sovereignty, Security and Democracy.	PM delivers keynote address at The Sydney Dialogue, speaks on India's technology evolution and revolution
Statement	Executive Vice-President-designate for Prosperity and Industrial Strategy	Today, India is the world's fastest-growing large economy, attracting global partnerships: PM
Statement	Statement at the European Parliament Plenary by President Ursula von der Leyen, candidate for a second mandate 2024-2029	Today India is working in every sector, in every area with unprecedented speed: PM at NDTV World Summit
Report	Report on the state of the Digital Decade 2023	Annual Report (Digital Governance) Ministry of Electronics and Information Technology
Report	EU strategic dependencies and capacities: second stage of in-depth reviews	Critical Minerals For India Report

4. The EU-India Relations in the Digital Age

In the evolving global landscape, relations and partnerships between the EU and India represent a significant dimension, especially considering the growing US-China rivalry and the growth of the importance of the digital realm. As two democratic powers positioned between the US and China, the EU and India have a common interest in shaping and regulating digital spaces.

This chapter will trace the development of the EU-India relations from early stages dominated mostly by economic ties, to a more strategic relationship that can be observed in the last few years. By understanding the historical context and current dynamics of this relationship, the paper will be able to better assess how the EU and India conceptualize and operationalize digital sovereignty in their partnership.

4.1. Historical Overview of EU-India Relations

Histories of the EU and India correspond in a certain way as both entities emerged after the Second World War. India gained independence from the United Kingdom in 1947 while the EU started its journey in the form of the European Coal and Steel Community (ECSC) in 1951. In 1957, the European Economic Community (EEC) was established, marking the beginning of the European Single Market known today.

The early days of the EEC were the time when the official relations between the Community and India were established. In 1962, the relations were established while in 1973, the EEC officially recognized India as a developing country within its Generalized System of Preferences (GSP) (*EU-India Relations | Bilateral Dynamics in an Evolving Global Order*, 2023, pp. 3–4). Integrating India into the GSP with the EEC was an important moment as the trade between the two increased significantly paving the way for deeper relations in the future.

Another important milestone came in 1981 as the Cooperation Agreement was signed. This agreement provided a formal framework and established mechanisms through

which collaboration in sectors such as trade, technology transfer, economic development, and cultural exchange were developed further (Ibidem, 4).

The 1990s were an especially fruitful period for the development of economic relations. Prior, the Indian economy was one of the most regulated economies in the world often labeled as the 'most autarkic non-communist country in the world' (Nayar, 1998, p. 335).

Although the reforms of the Indian economy started during the 1980s, the pace under which reforms were executed significantly increased after June 1991. Some of the key reforms included reforming the banking sector, removing licensing obligations for importers, lowering trade tariffs, and allowing the FDI to flow in higher quantities (Ibidem, 336). During the same period, the EU-India trade increased from $ 1.638 billion during the 1960s and 1970s to $ 5.701 billion during the 1990s (Kamath, 2022).

In 1993, the Maastricht Treaty was signed, marking the turning point in the history of the European Community as the European Union was established, tying European countries closer. During the same year, the Joint Political Statement between the Union and India was planned. In the next year, a cooperation agreement was signed between the EU and India raising the relations between the two beyond merely economic and trade relations (*The EU-India Joint Action Plan*, 2005). In other words, the Joint Statement and Plan opened the way for broader political alignment between the two.

The 1990s also marked a big change in the international sphere as the Cold War was over with the fall of the Berlin Wall. With the end of the Cold War, both the EU and India had specific challenges in front of them. On one hand, the just-transformed EU was occupied with spreading the European discourse across the new countries that were part of the Soviet bloc. On the other hand, India lost its partnership with the Soviet Union looking to expand its relations with the United States and establish itself as a nuclear power by acquiring the weapons in 1998 (Bava, 2021, pp. 367–370).

4.2. Strengthening the Partnership (2000-2013)

The turn of the century brought significant changes to the EU-India relations especially as the newly established European Union has established a new framework for foreign

policy. According to the new approach, the first EU-India summit was held in Lisboa, in 2000 (*EU-India Relations | Bilateral Dynamics in an Evolving Global Order*, 2023). The summit called for a 'new strategic partnership founded on shared values and aspirations' and came up with a 22-point action plan for achieving so (*28 June: EU-India Summit – POLITICO*, n.d.).

Despite the significant development of bilateral relations, the EU-India relations at the beginning of the 21st century can be characterized as mixed, with similarities and differences equally important.

The bilateral relations between the EU and India were still dominated by economic and trade issues with the EU remaining India's most important trade partner accounting for 21.6% of the country's trade (Wanger, 2008, p. 88). At the same time, the annual growth of the EU's exports to India was at 5.7% (Ibidem). Yet, certain questions about trade and investments remained open. During the 2000 Lisbon Summit, both parties recognized that their economic relations didn't reach their potential (*28 June: EU-India Summit – POLITICO*, n.d.).

Global issues were also shaped by converging and diverging views. Although both parties were advocating for a multilateral global system stressing the importance of the rule-based international system backed by the UN, their approaches to achieving so were different. The first one is related to the understanding of foreign policy. Indian foreign policy elites see India as a great power that pursues national interest and self-reliance-based policy in the first place (Wanger, 2008, pp. 88–89). Moreover, India sees itself as a singular state as opposed to the EU where multiple states are joined together to create the Union (Bava, 2021, p. 370). Ultimately, India's approach is based on classic Westphalian sovereignty while the EU is an entity that is transcending national borders and pooling sovereignty beyond national structures (Ibidem, 370).

After the Lisbon summits, the cooperation between the two was deepened in existing areas and expanded to new areas as the annual summits continued. During the fifth summit in Hague, bilateral relations were upgraded to a strategic partnership signed in 2004. In the context of the Hague Summit, the EU and India announced the signing of the Joint Action Plan in 2005 (JAP) deepened relations between the two in an

unprecedented way (*EU-India Relations | Bilateral Dynamics in an Evolving Global Order*, 2023).

The JAP stressed the importance of both entities sharing common values and aspirations towards democracy, pluralism, and human rights making them 'natural partners as well as factors of stability in the present world order' (Ibidem). The JAP is divided into five crucial areas of cooperation.

The most important provisions are the following:

1. The aim is to strengthen and further enhance high political dialogue between the two.
2. The provisions about 'effective multilateralism' where both actors expressed their belief in the multilateral system with the UN playing a central role.
3. Both parties stressed that the potential of EU-India cooperation in high-tech fields is huge.
4. Strengthening the Information Society dialogue with a focus on emerging fields such as 4G, e-commerce, internet governance, and universal service.

In this period, the cooperation was expanded into numerous areas such as low-carbon development, climate diplomacy, and development cooperation development. Low-carbon development became part of the agenda early resulting in big differences existing between the two. Only when the national legislation in India was changed in 2008 the cooperation became more fruitful resulting in numerous initiatives in climate change mitigation efforts (Jorgensen, 2021). Moreover, the cooperation in climate diplomacy was expanded while the Cotonou Agreement signed in 2000 by the EU and the group of African, Caribbean, and Pacific countries improved the visibility of the EU in India as a global player in economic development (Jayaram, 2021; Tripathi, 2021).

The JAP was an important point in the development of the EU-India relations due to the recognition of differences existing in terms of trade and investment sector. More precisely, the plan established dedicated working groups related to Intellectual Property issues, technical barriers to trade, and the correlated sanitary and phytosanitary issues. These issues later became the main difference regarding the free trade agreement negotiations officially called the Broad Based Trade and Investment Agreement (BTIA).

4.2.1. BTIA and the Emergence of Trade Issues (2007-2013)

The period between 2004 and 2007 can be marked as crucial in EU-India relations as cooperation was deepened in many sectors while trade issues that were pervasive in the period after emerged. Since that period, EU-India ties have experienced ups and downs as a lack of impetus on both sides prevented the achievement of previously planned goals (Panda, 2024, p. 21). Economic issues around the EU-India relations were high on the agenda with enhanced efforts to reach a free trade agreement but the positions between them were completely different at the moment of entering the negotiations.

Both sides started the negotiations with contrasting experiences of regional economic integration. More precisely, India's approach was predefined with foreign policy objectives as the trade policy was seen as a way to achieve foreign policy goals with little to no input of commercial interest (Kohler-Suzuki, 2021, pp. 152–155). Moreover, before entering the trade negotiations with the EU, India's experience was shaped predominantly by multilateral trade negotiations and, particularly, the free trade agreement signed with Sri Lanka in 1998 that marked the first bilateral trade agreement after 40 years (Ibidem, 153).

On the opposite, the EU as a *sui generis* actor has a different structure. In other words, foreign policy is regulated through the Common Foreign and Security Policy (CFSP) where member states (MS) prefer to focus on bilateral efforts. Accordingly, trade policy is shaped by the commercial interest of European industry while the competencies are in the hands of the EU and the European Commission (EC) leaving MS aside (Ibidem, 157-158). Finally, after the end of the Cold War, the priorities of the EU changed significantly as the Union tried to expand its influence globally and improve its economic position vis-a-vis the United States. When a multilateral effort to include so-called Singapore issues[2] in the World Trade Organization (WTO) in 1996, the EU changed its approach to bilateral (Ibidem).

Based on the report of the India-EU High-Level Technical Group (HLTG) and the joint commitments made at the 7th EU-India Summit in Helsinki, the official negotiations on BTIA started in Brussels in June 2007 (Prasad Srichandan, 2021). The report captured a

[2] The so-called Singapore challenges are the following: government procurement, trade facilitation, investment, and competition.

significant growth in trade volumes between the EU and India as the bilateral trade was growing at an average of 20% per year. Moreover, the trade in the service sector was growing at a rate of 10% annually with some differences existing in some specific service sectors such as legal, financial, and professional services (Kohler-Suzuki, 2021, pp. 158–166). Ultimately, the Group gave some recommendations before the negotiations started that were predominantly focused on the removal of duties, regulatory transparency, and public procurement (Ibidem, 163).

With such information, the negotiations began and were held in a total of 15 rounds covering issues such as trade in goods, services, investment, sanitary and phytosanitary measures, trade remedies, dispute resolution, and many others (Prasad Srichandan, 2021). However, the main point of discussion was the EU's demand for market access and tariff concessions in automobiles, wines, and spirits. The biggest problem, however, represented the fact that numerous Indian goods and products were already under duty-free or preferential treatment under the EU's GSP (Kohler-Suzuki, 2021, p. 157).

Moreover, policies between the EU and India were not compatible in many fields, especially in the ones crucial for the negotiations such as intellectual property rights, data security, registration of electronic products, agricultural exports, etc. The aforementioned differences caused the stall of the negotiations as the last meeting was held in May 2013 in New Delhi (Prasad Srichandan, 2021).

Ultimately, in the period between 2007 and 2013, several issues emerged as crucial factors contributing to the stall of negotiation. These issues can be summarized as follows (Kohler-Suzuki, 2021, pp. 158–171):

- **Tariff and Non-Tariff Trade Barriers.**

The EU pushed for tariff reductions on various goods, including automobiles, wine, and spirits. India's reluctance to lower tariffs in these sensitive sectors—especially the automobile industry, which was crucial for its industrial growth—became a significant roadblock.

Non-tariff barriers, such as regulatory transparency and standards, were also contentious. The EU sought harmonization with international standards, while India aimed to protect its domestic industries with specific regulatory frameworks.

- **Services and Professional Mobility.**

A major point of contention was the liberalization of services and the movement of professionals. India demanded easier access for its professionals to the EU, particularly in the IT sector, but faced resistance from some EU countries (especially the UK) due to immigration concerns. Visa policies and quotas for Indian workers remained unresolved, contributing to the suspension of talks.

The EU, on the other hand, sought greater access to India's financial services, legal services, and insurance sectors, which India hesitated to open up.

- **Foreign Direct Investment (FDI).**

There was a marked imbalance in FDI flows, with the EU being a significant investor in India but seeing minimal Indian investments in Europe. While the EU pushed for clearer rules and stronger protections for investors, India was cautious about overhauling its regulatory framework to accommodate foreign investors, particularly in sectors like retail and banking.

The core issues that plagued the BTIA negotiations were fundamentally about market access and regulatory protections, with both sides having different priorities. The EU aimed to gain greater access to India's growing market across various sectors, while India focused on protecting its industries and ensuring favorable terms for its professionals. Political and economic factors, such as immigration policies and regulatory disputes, further complicated the talks, resulting in the eventual suspension of negotiations in 2013.

4.3. Attempts to Put Negotiations Back on Track (2014-2022)

2014 marked an important year in the EU-India relations development as the general elections in India brought to power the Bharatiya Janata Party (BJP) and the new prime minister, Narendra Modi. From the start, the new government undertook an approach that caused disagreements on both sides. In the first place, specific incentives were adopted aimed at increasing the competitiveness of the key national industries and sectors. Some of these incentives are “Make in India”, “Skill in India”, “Digital India” and others (Hilpert et al., 2023, p. 2). In particular, the Make in India initiative was subject to disagreements as the Society of Indian Automobile Manufacturers (SIAM) started to strongly advocate for leaving the car industry outside of the BTIA as it would undermine the aims of the national manufacturing policy (Kohler-Suzuki, 2021, p. 172).

On the international level, the new Indian government under the BJP pursued a new approach that significantly hindered the possibility of getting negotiations with the EU back on track (Hilpert et al., 2023, pp. 2–8):

- India erected new import barriers and selectively increased critical tariff lines, which led to multilateral and bilateral conflicts. Besides the US, EU, and China, India had the most dispute settlements in front of the WTO.
- India’s reluctance to compromise on issues like agricultural subsidies hindered progress in the WTO negotiations.

Additionally, India's revised stance on foreign investment protections complicated the negotiations. In 2016, India unilaterally withdrew from several Bilateral Investment Treaties (BITs), including those with EU member states, signaling a shift toward a national model BIT framework (Ibidem, p. 6-8). This move aimed to mitigate investor disputes but raised EU concerns about the reliability of investment protections in India. Germany, a major investor in India, was particularly vocal, advocating for including investor protections in any comprehensive trade deal (Kohler-Suzuki, 2021, p. 162).

The political landscape also impacted the negotiation process. The Brexit referendum in June 2016 introduced uncertainties, as India had to reassess market access discussions previously framed under an EU-UK partnership. Simultaneously, bilateral trade discussions between India and the UK intensified, casting additional ambiguity on the structure and scope of a potential EU-India agreement (Ibidem, p. 164).

The EU also faced challenges in securing commitments on data security, a key issue in light of its General Data Protection Regulation (GDPR). India sought "data secure" status, allowing Indian firms to handle European data domestically. However, the EU required legislative assurances from India to meet GDPR standards (Ibidem, p. 167). This created a deadlock as India prioritized national regulations over the GDPR framework, delaying progress on digital trade integration.

In the concluding years of this period, India experienced several setbacks that slowed the progress toward continuing negotiations with the EU. In the first place, India was occupied with regional dynamics as the Chinese Belt and Road Initiative (BRI) became an important question in regional economic development. Moreover, direct bilateral tensions with China in 2017, 2020, and 2021 shifted the country’s attention more to the East (Sinha, 2022, p. 407). At the same time, in January 2017, a new Trump administration entered into the White House with a different approach to economic issues thus focusing on raising tariffs on Indian products and services in the US. Ultimately, the COVID-19 pandemic was a crucial issue for the Indian government in 2020 onwards since it showed how vulnerable Indian supply chains were (Ibidem, 407).

4.3.1. Common Denominator: Strategic Autonomy

The 22 previous years of EU-India relations and their efforts to negotiate were predominantly focused on gaining strategic track against each other and reaching more autonomous cases for their respective states and economies. Strategic autonomy is broadly defined as a nation or region's ability to function independently in critical areas, thereby reducing dependency on foreign actors and enhancing resilience (Lippert et al., 2019). Whether it was the negotiations on services, car production, or investment, the bilateral relations between the EU and India were centered around autonomy issues.

This goal has been underscored by events such as the COVID-19 pandemic, geopolitical tensions, and shifting economic landscapes, each highlighting vulnerabilities in global supply chains and digital infrastructure. For both the EU and India, these disruptions revealed the importance of achieving greater self-sufficiency and sparked new policies to protect and develop their respective economic and digital realms.

Key factors driving the EU and India toward strategic autonomy include the vulnerabilities exposed by COVID-19 and an increasingly polarized global political environment. The pandemic, which disrupted supply chains worldwide, highlighted critical dependencies on external suppliers, prompting both the EU and India to re-evaluate their reliance on foreign goods and technologies. In India, the COVID-19 pandemic only reemphasized the country's supply chain gaps during the pandemic and underscored its need for self-reliance in manufacturing and technology, reinforcing initiatives like "Make in India" and "Digital India" to strengthen domestic production and digital infrastructure (Kohler-Suzuki, 2021, p. 172). The EU faced similar imperatives, where dependency on foreign tech giants, particularly in the digital sector, spurred policy actions aimed at building a secure and self-sufficient digital ecosystem (Christakis, 2020).

To add to the previous point, the surge of the digital realm in 2017, 2018, and particularly after 2020, added another layer to strategic autonomy thinking. Overall, the information and communication technology sector (ICT) grew by an average of 6.3% annually between 2013 and 2023 outpacing many OECD countries (OECD, 2024). Moreover, business e-commerce sales saw a remarkable increase, rising nearly 60% from $17 trillion in 2016 to $27 trillion in 2022 across 43 countries reflecting the shift towards digital transactions accelerated by the pandemic (Digital Economy Report 2024, 2024). Ultimately, investment in generative AI skyrocketed from $1.3 billion in 2022 to $17.8 billion in 2023, highlighting a growing focus on AI technologies within the digital economy (OECD, 2024).

In the digital realm, data sovereignty is a focal point of this push for strategic autonomy. Both the EU and India are acutely aware of the need to control and secure data flows within their territories. The EU's GDPR sets a stringent framework for data privacy, intended to protect European citizens' data from misuse by non-EU entities. India, for its

part, has pursued its path with the National Digital Communications Policy (NDCP, 2018) stressing that “digital infrastructure and services are increasingly emerging as key enablers and critical determinants of a country’s growth” (Ibidem, p. 1).

As a consequence, both the EU and India face similar challenges in reconciling national strategic autonomy with the demands of global trade. For both, the pursuit of self-reliance is not only a defensive measure but a proactive step toward building resilient economies capable of withstanding global disruptions. This shared focus on autonomy provides a foundation for potential cooperation in the digital realm, as both regions explore frameworks for digital governance, data security, and cybersecurity standards. The next section delves into the evolving EU-India digital relationship, focusing on how strategic autonomy influences their approaches to digital trade, data regulations, and technological sovereignty.

4.4. Toward a Digital Partnership: New Dimensions in EU-India Relations

The last couple of years were predominantly shaped by the intensification of the geopolitical rivalry between the US and China which also had a significant impact not only on the EU-India relations but also on broader alliances and partnerships. The U.S.-China rivalry has been marked by trade disputes, technological decoupling, and competition for supremacy in emerging technologies such as generative AI, 5G, and quantum computing. The U.S. has imposed restrictions on Chinese technology firms, citing national security concerns, while China has advanced its "Digital Silk Road" initiative, expanding its technological influence globally. These developments have heightened concerns among democracies, including the EU and India, about over-reliance on Chinese technologies and the risks of cyber surveillance and authoritarian influence (Blackwill, 2024).

Russia's invasion of Ukraine in 2022 added another layer of complexity. The conflict highlighted the importance of secure digital infrastructure and resilience against cyberattacks, as evidenced by the role of cyber warfare in the conflict. It also reinforced the need for stronger partnerships among democracies to counter authoritarian regimes

and build secure technology ecosystems (Haass, 2022). Both the EU and India have faced pressure to navigate their relationships with Russia carefully, given Europe's energy dependence and India's long-standing defense ties with Moscow (Ibidem). Despite these challenges, the shared imperative of reducing reliance on authoritarian regimes has drawn the EU and India closer in the digital domain.

In such a geopolitical context, the principal goal of states worldwide has become to reach strategic autonomy and decrease exposure to dependencies (Kranenburg & Okano-Heijmans, 2023b, p. 5). Furthermore, international economies and trade are increasingly shaped by cross-border services and data transfers which are used as inputs in the production of other goods and services (India and the European Union in 2030: Building a Closer Economic Relationship, 2023, p. 74) bringing technology to the center of geopolitical goals of states globally.

In response to these geopolitical shifts, the EU and India have both sought to strengthen their digital partnership. India has been actively participating in different platforms aimed at trade and technology issues. One of them is Quad initiative (Quadrilateral Security Dialogue) which represents the platform between the US, India, Japan, and Australia to enhance their cooperation in the field of emerging technologies (Ankita, 2024). Besides the Quad Initiative, India sought to expand its partnership in emerging technologies separately with the US and Australia (Ibidem).

The EU, on the other hand, is trying to develop a series of digital partnerships with Asian countries including Japan in May 2022, South Korea in November 2022, and Singapore in February 2023. The labelled these partnerships as critical for creating a digital world according to its standards that will be pursued with cooperation with like-minded countries (Ibidem). Although the partnership between the EU and India seems natural in the international arena due to their democratic orientation and similar positions, there are, however, certain discrepancies in their digital relations, particularly in the vision and the approach that both entities have for it.

The following analysis of policy areas with potential of cooperation has been derived from reading of official documents, secondary literature, and critical commentaries on materials all together.

4.4.1. Mutual Interests and Diverging Views in the EU-India Relations

The relations between the EU and India in the digital realm have been limited before the establishment of the Trade and Technology Council (TTC) in 2022. Since then, the relationship has entered a new phase especially because of the importance of India in international relations (Nachiappan, 2024, pp. 27–28). According to Kartnik Nachiappan, India represents a strategic swing state in the field of digital regulation meaning the orientation towards a more liberal or more authoritarian digital stance could have significant consequences on the international system (Ibidem, 27).

Following this argument, the introduction of TTC marks an important moment not only because it represents the start of broader EU-India relations in the digital realm but also because it has huge potential to bridge the existing gaps in the crucial aspects of digital relations. To identify these gaps, this thesis will follow the division of digital relations according to the main policy areas in the field developed by Kartnik Nachiappan (Ibidem, 27-33). These policy areas are Cybersecurity, AI, 5G, 6G, Data Governance, and semiconductor technology development. At the same time, these policy areas represent the main arenas in which both the EU and India are trying to establish their sovereignty, marking the core of digital sovereignty discourse. At the same time, all of these technologies represent the areas within the scope of TTC that have three working groups: strategic technologies, green and technology, and resilient supply chains (Delivorias, 2024).

Before diving deeper into these exact policies, one important note should be made. Both the EU and India perceive themselves as liberal democracies inclining naturally to the free flow of information and protecting freedom (India and the European Union in 2030: Building a Closer Economic Relationship, 2023, p. 75). Moreover, both countries see regulatory protection as necessary when speaking about the digital world (Ibidem, 75) but the difference comes from the method of achieving so. The EU is more centered around the protection of citizens and fundamental rights while India predominantly focuses on economic security and the capability of its economy to progress (Bharti & Singh, 2024).

In the rest of the chapter, each of these policy areas will be analyzed to present similarities and differences in both the EU's and India's approaches. Ultimately, TTC will be introduced as the potential arena where views on these policy areas are confronted.

Cybersecurity

Both the EU and India recognize the importance of cybersecurity, the main differing factors come from the nature of threats they are facing and the maturity of their infrastructure.

The EU's approach to cybersecurity is mainly centered around Russian activities in cyberspace as, according to the head of the EU Agency for Cybersecurity (ENISA), the number of attacks has increased significantly after the Russian invasion of Ukraine in February 2022 (Derek, 2024). Accordingly, the EU's approach is mainly focused on protecting its citizens and critical infrastructure from attacks from Russia that are trying to destabilize the EU to decrease the support the Union gives to Ukraine (Ibidem).

On the other hand, India is faced with a different type of problem, namely its digital infrastructure which has been outpaced by the country's fast development in the digital domain (Choudhary, 2023). Moreover, India is being challenged by numerous state and non-state actors targeting its national infrastructure.

While both countries have focused on deterring cross-border cyber attacks, the normative approaches each of them has undertaken differ significantly (Nachiappan, 2024, p. 29). While India has been actively advocating for strong state authority in matters, the EU focuses more on the set of non-binding norms and principles for responsible state behavior online (Ibidem, 29).

Artificial Intelligence (AI)

Both the EU and India are pursuing regulation of AI in their domestic arenas; the main differing view is appearing on the principles behind regulation. The EU's approach is centered around the protection of democracy, fundamental rights, and the rule of law. In other words, AI technology is seen as a very potent weapon but, at the same time, very

dangerous, and it needs to be regulated to protect citizens at all cost (Bharti & Singh, 2024).

As a part of its digital strategy, in June 2023, the EU adopted the first-ever AI regulation aimed at making AI technology safer and more transparent for citizens (*EU AI Act*, 2023). This regulation follows the overall EU stance on artificial intelligence that is predominantly centered around risk mitigation and protection of fundamental rights (Ibidem). On the contrary, India's approach follows a different logic from the perspective of the goal behind the policies adopted. More precisely, strict regulation is seen in India as a barrier to promising companies and start-ups as limitations put on AI technologies may hinder the country's economic growth (Bharti & Singh, 2024). The main principle behind India's approach is centered around protecting the innovation capacity of the country's economy rather than protecting its citizens as is the case with the EU AI Act (Ibidem).

Data Governance

The situation within the data governance field follows the logic behind AI and cybersecurity fields. In May 2018, The General Data Protection Regulation (2018) came into force marking the beginning of what Anu Bradford called "the Brussels effect" (Rakesh, 2022, p. 111). Namely, the effect is centered around other countries, both developed and developing ones adopting the EU-inspired legislation on data governance (Ibidem, p. 111). Having that said, the Brussels effect exports the data governance framework adopted in the EU which is based on a human-centered approach and the protection of rights and standards (Nachiappan, 2024, p. 28).

The Indian approach, on the contrary, is based on security and control, not personal and community rights (Ibidem, p. 28). Moreover, India is developing a data governance framework that is located in the balance between privacy, economic growth, and national security (India and the European Union in 2030: Building a Closer Economic Relationship, 2023, p. 75). According to these principles, the first data protection legislation was adopted in India in 2018 through the Personal Data Protection Bill which was withdrawn shortly after (Rakesh, 2022, p. 113). The provisions of the Bill stated that all copies of all personal data had to be stored in India with limitations on

data crossing borders (Ibidem, 113). In 2023, India adopted a new Digital Personal Data Protection (DPDP) that facilitates the transfer of data between India and 'trusted jurisdictions' without clearly defining what a trusted jurisdiction is (Nachiappan, 2024, p. 28).

The lack of clear data protection rules in India poses a double threat to the EU-India digital relations. In the first place, with the US companies lobbying heavily for such a void in legislation, the lack of data protection in India could hinder the bilateral trade agreement negotiations. Secondly, the non-existence of clear provisions complicates data exchange between the two countries marking a significant hurdle in economic and business relations (India and the European Union in 2030: Building a Closer Economic Relationship, 2023, p. 77).

5G and 6G Technologies

Regarding the 5G and 6G technologies, approaches followed by the EU and India differ mainly in their relation to Chinese conglomerate, Huawei, as one of the cheapest communication providers (Nachiappan, 2024, p. 30). After the Sino-Indian border clashes, India decided to pursue the approach centered around European and domestic providers while at the same time trying to develop its domestic 6G network (Ibidem, p. 30).

The EU, on the contrary, decided to adopt the 5G technology provided by Huawei despite security risks. At the same time, the joint development of 6G technologies has been pursued through cooperation with US companies and the TTC with the US (Ibidem, p. 30).

Semiconductors

In the semiconductor field, both the EU and India are pursuing the goal of becoming global technological leaders in the field. Through large-scale investment packages such as the European Chips Act in the case of the EU, and Semicon in the case of India, both countries are trying to lower their dependencies and increase resilience in the field (Ibidem, p. 31-32).

4.4.2. Open Questions - The Road to TTC

The digital relations between the EU and India, influenced significantly by global geopolitical rivalry and technological competition, highlight both shared goals and existing gaps. The intensifying U.S.-China rivalry has driven democracies like the EU and India to reconsider over-reliance on Chinese technologies, emphasizing the need for secure and autonomous digital infrastructure. According to Katasthane, successful international partnerships require a convergence of interests, a broad alignment of values, and complementarity in strengths (Katasthane, 2023, p. 50). In the technology field, the EU and India are aligned regarding all three parameters.

In the first place, both actors adopt distinct strategies to achieve digital sovereignty. Furthermore, both partners are concerned with digital sovereignty and power distribution in the world. The EU emphasizes citizen protection, fundamental rights, and reducing dependency on authoritarian regimes, while India focuses on fostering economic security and advancing its technological capabilities. Although having different priorities, both of the actors share the same values (Ibidem, 50).

Key divergences manifest across policy areas like cybersecurity, AI, data governance, and 5G/6G technologies. The EU's regulatory framework prioritizes safeguarding critical infrastructure and citizen rights, driven by external threats like Russia. Conversely, India confronts challenges stemming from the rapid growth of digital infrastructure and the need to counter threats from neighboring regions. Similarly, the EU's AI regulations emphasize ethical use and citizen rights, while India's approach fosters innovation by minimizing regulatory barriers, and prioritizing economic growth.

Last but not least, the complementarity between the two exists in the way that India brings human capital while the EU brings expertise, infrastructure, and capital to the table (Ibidem, 50).

4.5. The EU-India Trade and Technology Council (TTC)

Having in mind the already existing interests of the EU and India, TTC has the potential to be a forum for technological discussion and a place where further relations are deepened. From the perspective of India, TTC possesses a crucial potential for the country's weak points. In the first place, the domestic innovation and R&D efforts in India are very limited resulting in the private sector not gather large amounts of investment. In fact, 70% of investment in innovation comes from government funds (Chaundhri, 2023, p. 38). As the EU possesses a stronger private sector regarding innovation investment, TTC could potentially serve as the arena where investment deals are made.

Moreover, the geopolitical situation in the world puts India in the perfect position to expand its cooperation with the EU. After 2020, the relations with China have undergone serious changes as border conflicts resulted in the removal of China as one of India's main partners especially in the technology sector (Ibidem, 38-39). At the same time, the US sees India as the strategic partner next to the EU in creating a coalition that would go against the Chinese infrastructure and data governance model (Ibidem, 39-40). On the other hand, from the EU's perspective, TTC serves as the potential arena for acquiring broad technological partnerships with India but also serves as the place where 27 member states with different interests can have one voice (Ibidem, 43).

4.5.1. TTC, Digital Sovereignty and Constructivist Theory

From a constructivist perspective, the EU-India TTC operates as the arena where digital sovereignty is not only articulated but actively constructed through interaction and discourse. Constructivist theory emphasizes that sovereignty, including its digital variant, is not a fixed attribute but a socially constructed concept that evolves through shared norms, values, and practices (Adler, 2013). The TTC, with its structured working groups and ministerial meetings, exemplifies a platform where these processes unfold, allowing the EU and India to negotiate and co-create meanings of digital sovereignty.

Within the TTC, digital sovereignty is not a pre-existing consensus but a contested and negotiated concept. The EU's discourse often frames sovereignty in terms of strategic autonomy and regulatory frameworks, such as the GDPR, which prioritizes data protection and technological independence. Conversely, India's narrative emphasizes self-reliance, data localization, and protection against external technological dependencies. Constructivist insights suggest that these differences do not hinder collaboration. Instead, they provide the groundwork for a dynamic process of norm-building (Gammeltoft-Hansen & Adler-Nissen, 2008).

The ongoing ministerial meetings and their outcomes demonstrate how digital sovereignty is iteratively defined and refined. Constructivist insights showcase that sovereignty claims are not static but that they evolve as actors engage in dialogue and respond to external pressures.

To respond to the second research question on whether TTC can bridge the existing gaps on the digital sovereignty understanding, the requirement is to first analyze its structure and ministerial meetings held till the moment of writing.

4.5.2. The Structure of the TTC and Ministerial Meetings

TTC was officially announced by the President of the EC, Ursula von der Leyen, and the Prime Minister of India, Narendra Modi, on the 25th of April in New Delhi. On the EU side, TTC will be co-chaired by Executive Vice-Presidents Margrethe Vestager and Valdis Dombrovskis, while on the Indian side, the co-chairs will include Subrahmanyam Jaishankar, Minister of External Affairs, Piyush Goyal, Minister of Commerce and Industry, and Ashwini Vaishnaw, Minister of Electronics and Information Technology (*EU-India: New Trade and Technology Council*, 2023).

While the ministerial work will occur between the officials of the EU and India, the preparatory work will be done by three working groups on which TTC is based. Three working groups are the following (Ibidem):

- **Strategic technologies, digital governance, and digital connectivity -** The group will collaborate on shared interests like digital connectivity, AI, 5G/6G,

quantum computing, semiconductors, cloud systems, cybersecurity, digital skills, and platforms.

- **Green & clean energy technologies -** This group will focus on green technologies, emphasizing investment, standards, and innovation in areas like clean energy, circular economy, waste management, and ocean pollution.

- **Trade, investment, and resilient value chains -** The group will focus on supply chain resilience, access to critical materials, and energy, addressing trade barriers and global challenges through multilateral cooperation and promoting international standards.

At the moment of writing, two ministerial meetings were held. The first TTC meeting in May 2023 in Brussels focused on collaboration in semiconductors, digital infrastructure, clean energy, and supply chains, with a work plan for e-mobility, battery recycling, and standards. On the sidelines of the first meeting, FTA negotiations were showing the importance of the TTC not only for the EU-India digital but also overall relations (*India - EU TTC Working Group 2 (WG2) on "Green & Clean Energy Technologies,"* 2024).

The second ministerial meeting of the India-EU TTC was held virtually on November 24, 2023. Co-chaired by India's External Affairs Minister Dr. S. Jaishankar, Commerce Minister Shri Piyush Goyal, and Electronics and IT Minister Shri Ashwini Vaishnaw, along with EU Executive Vice-Presidents Valdis Dombrovskis and Vera Jourova, the meeting reviewed progress in areas like semiconductors, high-performance computing, digital public infrastructures, electric vehicle batteries, and resilient supply chains. A significant outcome was the signing of a Memorandum of Understanding on semiconductors, aiming to enhance the resilience of semiconductor value chains between India and the EU (Ibidem). So far, three working groups have achieved the following results (Delivorias, 2024):

- **First Working Group -** For now, the first working group launched three initiatives; one in the field of AI, in a multi-stakeholder setting with the goal to bridge the gap between theory and practice on AI. Second initiative focuses on semiconductors and its exploring the ways in which both the EU and India can reduce their vulnerabilities in the sector.

- **Second Working Group -** Through this group, the EU and India confirmed their commitment for net-zero and sustainability policies. Moreover, they agreed that the following areas are essential for their cooperation: renewable and low-carbon hydrogen, batteries for electric vehicles and standards for them. Some other important areas are marine plastic and pollution, the reduction of wastewater.

- **Third Working Group -** The final working group is focused on supply chains and mechanisms around FDI screening. Some of the key areas under the group's jurisdiction are market issues around trade barriers and the creation of resilient value chains.

5. Comparative Digital Sovereignty Analysis in the EU-India Relations

After laying the groundwork in the previous chapters, this chapter will focus on the application of the research framework to the sample of documents presented. As outlined before, there are two research questions of this thesis: 1) To understand how the EU and India conceptualize and operationalize digital sovereignty, and 2) To what extent does the TTC serve as a platform for addressing and potentially harmonizing different digital sovereignty discourses.

Each document from the sample will be presented one by one, conducting phases 1 and 2 of the analytical framework. In phase 1, documents will be analyzed to see whether they contain a significant discourse of digital sovereignty assessed through three criteria previously presented: centrality, applicability, and relevance (Table 3.1). If the document passes all three criteria, the document proceeds to phase 2 to analyze which type of digital sovereignty discourse is contained. To do so, each document will be analyzed through their responses to three questions about main adversaries, policy goals, and methods used for achieving digital sovereignty (Table 3.2).

Table 3.1 - Filtering materials with significant digital sovereignty discourse

Criterion	Definition
Central	Materials contain problems/challenges related to the digital sphere and the term digital sovereignty and alternative concepts that have the highest frequency in them.
Relevant	Materials contain proposals that are expected to address problems/challenges identified and are feasible to solve.
Applicable	Materials specify strategies and steps on how digital sovereignty discourse should solve the problems/challenges identified.

Table 3.2 - Analysis of Digital Sovereignty Discourse

Question 1	Who or what is seen as the problem?	
Answers	Digitalization	Tech Platforms/Big Tech
Value	1	2
Question 2	What is the goal of the Digital sovereignty discourse?	
Answers	Competitiveness	State Security
Value	1	2
Question 3	What are the means proposed as a solution?	
Answers	Standardization/Regulation	Protectionist Measures
Value	1	2

Upon completion, the results will be quantified to reach the type of digital sovereignty discourse present in every document: security-oriented or economically oriented digital sovereignty discourse.

Table 3.3 - Acquiring Results

Value	3,4	Economic DS	Creating an economic context that favors technological innovation within the national territory. Fostering autonomy of the national economy concerning foreign technology and service providers.
	5,6	Security DS	Emphasis is put on controlling digital infrastructure within national borders and tackling constant monitoring of citizens performed by foreign countries, namely the US.

As the results are quantified and obtained, TTC analysis will be introduced to complete the results and the response to the second research question.

5.1. The EU Digital Sovereignty Documents Analysis

The EU Artificial Intelligence (AI) Act

The AI Act was officially signed in June, 2024 while it came into force in August the same year. It was labelled as the first comprehensive regulation of artificial intelligence in the world (Madiega, 2024). The act follows a structural, risk-based approach based on the potential impact of the AI systems on the European market where systems are

divided into four categories: minimal risk, transparency risks, high risks, and unacceptable risks (Ibidem, 8).

However, the AI act was adopted with different receptions both on the EU level and globally. On the EU level, various stakeholders expressed their concerns with the act, especially in terms of cost. Small and Medium Enterprises (SMEs) are particularly vulnerable to this cost as it will be hard for them to sustain the cost. Globally, key issues that emerged were centered around terminology used in the act that are crucial for harmonisation of AI regulation (Ibidem, 11).

Identifying Digital Sovereignty Significance

By applying centrality, relevance, and applicability criteria on the AI Act it brings the result of the significant digital sovereignty discourse present in the document. Starting with the centrality of the discourse, the Act contains clear issues pertaining to digital sphere digital sovereignty or alternative concepts are used to present to describe the issue (AI Act, 2024). Although the term digital sovereignty is not mentioned specifically, the act clearly mentions that issues happening in the digital sphere should clearly be under jurisdiction of the EU authorities even if the entity providing AI systems is not located on the EU's territory (Recital 45). Moreover, any system that personalizes digital solutions (Recital 22) or affects critical digital infrastructure (Recital 55) falls under the scope of the Act.

In addition, sovereignty in digital spaces is seen as a relevant concept since the attempt of the EU to transfer their sovereignty to digital spaces where even actors outside the Union will have to comply with the rules needed (Recital 45). The specific attention is given to General-purpose AI systems. Whether provided internally or externally, the developers of the system must comply with the Eu regulations (Recitals 85).

Finally, the whole Chapter VII of the Act (Articles 64-70) contains provisions on specific actions that the EU will pursue to solve issues related to sovereignty in terms of AI systems. These provisions establish AI Office (Article 64), the European AI Board (Article 65), and Advisory Forum (Article 67), among others, aimed at developing the EU-based governance structure that will ensure that entities providing AI systems in the

EU will respect the EU rules. In other words, the discourse of digital sovereignty is applicable to the issues identified.

In summary, the AI Act, although not using the concrete term digital sovereignty, contains provisions directly related to it. More specifically, it ensures that the AI systems operating in the digital sphere that are able to trespass borders of the EU more easily will still need to comply with EU regulations and respect its fundamental rights values.

Thematic and Narrative Analysis

The thematic analysis of the digital sovereignty discourse in the AI Act gave the following results (Table 4.1).

Table 5.1 - AI Act Thematic Analysis

Who or what is seen as the problem?	Tech Platforms/Big Tech	2
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Standardization/Regulation	1

Although mentioning digitalization, the AI Act focuses predominantly on the private actors that are providers of AI systems. More precisely, the representatives of these actors from third countries must be appointed to represent these companies within the European Commission or other designated bodies (Article 22). These representatives are required for all types of AI systems regulated by the act and will serve as contact points between the Union and companies.

The question about the competitiveness and state security requires additional attention as the first recital states that the aim is “to protect [the EU] against the harmful effects of AI systems in the Union, and to support innovation” (Recital 1). Accordingly, the distinction between the two is not very clear.

However, the following arguments support the state security discourse-type:

- Risk-based approach. The structure of the Act is centered around specific obligations for AI developers based on how risky these systems are for the Union's security (Chapter 3-5).
- The AI governance structure presented in Chapter 7 is centered around trustworthy and safe deployment of systems in the EU market. In other words, the AI Act is primarily concerned with the increased trustworthiness of AI that would, subsequently, result in greater economic competitiveness of the EU.

Ultimately, the answer to the question about the solution is standardization/regulation. As shown, the aim of the act is to provide a regulatory framework for AI developers to respect in order to deploy their systems on the EU market.

Total score: 5. With the total score of 5, the digital sovereignty discourse in the AI Act by the EU is security oriented. As discussed before, the essential aim of the act is to develop a safe and trustworthy environment for deployment of AI systems. The AI act is also fostering innovation by providing measures for startups and SMEs (Article 62) but the core aspect is the Union's security since actors developing AI in third countries are bound with heavy regulation and presence of their representatives in Brussels ensuring smooth cooperation with authorities.

2030 Digital Compass: The European Way for the Digital Decade

The European Way for Digital Decade strategy was adopted in June 2022 as the key policy document to address the twin transition, green and digital. The Strategy follows the corporate principle outlining the safe framework for IT solutions and innovation (Bahrke, 2022). As a key strategic document for the digital development of the EU, this strategy is specifically focused on digital sovereignty and autonomy (*2030 Digital Compass: The European Way for the Digital Decade*, 2021). The document lays down four concrete steps to achieve goals presented while also presenting a few Key Performance Indicators (KPIs) to track the progress (Ibidem, 4-12).

Identifying Digital Sovereignty Significance

The digital sovereignty discourse is present in the document in both direct and indirect ways. In the first place, the document specifically mentions and recognizes digital sovereignty as one of the essential goals for the EU (Ibidem, 1). Indirectly, the document specifies the problems in digital spaces that are directly related to digital sovereignty thus fulfilling the criteria of centrality. More specifically, the COVID-19 pandemic clearly demonstrated the possible benefits of digitization of the economy, but at the same time, showcased some of the strategic vulnerabilities of the Union (Ibidem, 1-2).

Accordingly, the discourse of digital sovereignty shows a high relevance in the document as proposals laid down are connected to the discourse. To specify, sovereignty in digital spaces is seen as a predicament to solving issues such as data storage where data created by EU citizens is exported outside of the EU (Ibidem, 5-7). Moreover, critical technologies such as quantum computing, microprocessor and chip production used in the EU are predominantly produced outside of the EU laying down the strategic vulnerability of the Union (Ibidem, 7-8).

Ultimately, the document lays down the concrete 4-step strategic framework for achievement of digital sovereignty in designated fields along with several KPIs for tracking the progress. In other words, the discourse of digital sovereignty is highly applicable for the document as the creation of EU-based clouds for data processing, domestic digitally skilled workforce, domestic capabilities for quantum computing, among others, are prescribed as solutions to recognized challenges.

Thematic and Narrative Analysis

The strategy contains provisions that could position it on both sides of the spectrum for each question. The results are presented in the table below (See Table 5.2).

Table 5.2 - The EC Digital Strategy Thematic Analysis

Who or what is seen as the problem?	Tech Platforms/Big Tech	2
What is the goal of digital sovereignty discourse?	Economic Competitiveness	1
What are the means proposed as the solution?	Standardization/Regulation	1

The strategy specifically mentions digitalization in the context of COVID-19 pandemic that showcased how digital technologies have become essential for businesses across the Union (*2030 Digital Compass: The European Way for the Digital Decade*, 2021, p. 8). Moreover, the document recognizes the importance of digitalization beyond the business sector as "digital technologies are now imperative for working, learning, entertaining, socialising, shopping and accessing everything from health services to culture" (Ibidem, 1).

At the same time, the document refers to the economic competitiveness being under pressure because of reliance on a few big tech companies that are based outside of the EU (Ibidem, 2). Although both are mentioned, big tech companies are seen as the main problem because of the following reasons: 1) digitalization is not seen as a problem but as an opportunity to further enhance the growth of the EU economy, and 2) the document is based on a 4-step strategy that is aimed to develop digital capabilities of the EU and thus, compete big tech companies often located out of the EU.

The presented arguments also support the response to the second question as economic competitiveness has been the key pursuit of the strategy. More precisely, of the 4 steps upon which the strategy is based, 3 are directly related to the competitiveness of EU-based companies (Ibidem, 4-12). The remaining step, "Secure and performant sustainable digital infrastructures" (Ibidem, 5) covers the area of state security but solely for the purpose of economic competitiveness. Put simply, digital infrastructure is seen as "a prerequisite for a society in which every business and citizen can fully participate" (Ibidem, 5).

Finally, the third question is the most difficult to answer as the distinction between the actions proposed is not very clear. However, the protection of the EU economy is,

according to the document, planned to be achieved by setting clear rules for the entities operating inside the Union. The strategy specifically follows some of the key initiatives EU adopted or is adopting for the digital space such as Digital Services Act (DSA), Digital Markets Act (DMA), and Data Governance Act (DGA) (Ibidem, 2). All of these initiatives aim to establish rules to ensure fair competition and reduce dependence on external providers through standardization and governance measures.

Total score: 4. The assessment showed that the European Way for Digital Decade strategy is more oriented towards economic digital sovereignty discourse as it focuses on laying down the measures favorable for innovation of companies inside of the EU. However, the discourse leans towards more security oriented digital sovereignty only by distinctive focus on big tech companies as the problem.

A European Strategy for Data

The European data strategy was adopted in 2020 at the same time as the Digital Commission document representing another key pillar of the EU digital strategy (*A European Strategy for Data*, 2020). Seeing data as the cornerstone of currently ongoing digital transformation, the strategy focused on developing the framework that will allow the EU and its citizens to capture a piece of value of this transformation (Ibidem, 1). As the Digital Commission strategy presented above, the European Data strategy is divided into 4 essential steps (Ibidem, 12-23).

Identifying Digital Sovereignty Significance

This strategy clearly outlines the notion of strategy autonomy, a concept highly closely connected to the digital sovereignty discourse and that represents the alternative concept to it. Challenges identified are present in the digital sphere as the strategy outlines how the EU could capture the value of the economy being transformed to the digital one (Ibidem, 1-2). Moreover, the challenges stated are a result of the lack of capacities inside of the EU to store and process data of the EU citizens (Ibidem, 8). In other words, the data produced in the EU and by the EU citizens needs to be stored, processed and captured inside of the EU, which represents the clear notion of sovereignty in digital spaces. Thus, the centrality criteria is fulfilled.

The document also puts out a specific strategy to solve the issue that is closely connected to digital sovereignty. In particular, the ground for the investment in strategic infrastructure is set. The investments are aimed at building European capabilities of managing, processing and storing data outside of the current framework in which mostly a few external actors are running the system (Ibidem, 9-10).

The strategic framework presented in the document, thus, gives a clear strategy on how digital sovereignty should solve the issues related with data produced in the EU. Ultimately, the European strategy contains a digital sovereignty discourse that is highly significant.

Thematic and Narrative Analysis

The European Strategy for data contains a clear aim towards enhancement of the EU's economic competitiveness but, at the same time, provides challenges in identifying what is the main problem that needs to be addressed. The results are presented in the table below (Table 5.3).

Table 5.3 - A European Strategy for Data Thematic Analysis

Who or what is seen as the problem?	Digitalization	1
What is the goal of digital sovereignty discourse?	Economic Competitiveness	1
What are the means proposed as the solution?	Standardization/Regulation	1

The distinction between digitalization and Big Tech companies as the main challenge is not clearly articulated in this document. On a few occasions, the document stresses the concentration of market power present within the companies operating in the data processing and storage market (*A European Strategy for Data*, 2020, p. 9). In particular, the share of the EU-based companies in the market is seen as not sufficient. Even though the market concentration and Big Tech are clearly mentioned, the document sees digitalization as the issue. To make it more specific, unregulated digitalization is the problem in which the bigger players outside the EU are benefiting the most.

Accordingly, the strategy laid is focused on regulating the data storage and processing inside of the EU that will improve the capabilities of local companies to use that data and be more competitive in the market (Ibidem). Ultimately, the strategy lays down a regulation through which the companies from third countries need to operate in the EU market.

Total score: 3. The European Data strategy is the document that contains a clear digital sovereignty discourse that is economically oriented. Although other aspects, such as cyber security or actions related to the Big Tech are mentioned, the undisputed aim of the strategy is to improve economic competitiveness of the EU-based companies.

European Commission Digital Strategy: Next Generation Digital Commission

The European Commission digital strategy is a document that deals with the digital transformation of the EC as the main executive body of the Union. The strategy, adopted in 2022, contains five key strategic objectives to achieve the digital transformation of the body (*European Commission Digital Strategy Next Generation Digital Commission*, 2022). Although the document contains the word digital sovereignty, the document doesn't contain the discourse of digital sovereignty making it a particular case in our study.

Identifying Digital Sovereignty Significance

The problems presented in the strategy are related to digital and the term digital sovereignty is present but the overall goal of the document is not to improve digital sovereignty of the EU. On the contrary, the goal is to redefine the actions and the organization of the EC in digital spaces so that the body could fit into the emerging digital economy (Ibidem, 1).

Total score: Digital sovereignty discourse is not significant. Digital sovereignty is mentioned as one of the ten principles making it just a portion of the discourse and not central. The solutions presented are relevant and applicable since they include building an infrastructure that would allow the EC to operate more autonomously, but the central theme of the document is related to digital sovereignty.

The EU's Cybersecurity Strategy for Digital Decade

Adopted in 2020, the EU's cybersecurity strategy reflects on the new challenges related to the digital sphere as a result of the global COVID-19 pandemic (*The EU's Cybersecurity Strategy for the Digital Decade*, 2020). As the strategy suggests, many economic sectors including business, large industry, welfare, etc. have transferred their operation to digital spaces. Although beneficial, the increased presence in digital spaces brough new threats in the form of cybersecurity threats.

Accordingly, the strategy lays down a strategic framework aimed at lowering down the negative effects of those threats as well as the policy instruments and regulation to follow it.

Identifying Digital Sovereignty Significance

The EU's Cybersecurity strategy is located between the global and European approach. Although provisions contained in the strategy are mostly connected to European problems, a significant part of them deals with increasing global cybersecurity by saying "thinking global, acting European" (Ibidem, 4). In more detail, the EU's action in the cybersecurity sphere is centered around three key pillars (Ibidem, 4): 1) resilience, technological sovereignty, and leadership; 2) building operational capacity to prevent, deter, and respond; and 3) advancing a global and open cyberspace.

Moving on the criteria, the strategy contains the significant digital sovereignty discourse as the discourse present is central, relevant, and applicable. Regarding centrality, the issues presented are related to digital and cyberspace and, at the same, technological sovereignty is presented as one of the key pillars of the document (Ibidem, 5). Not only that the discourse is central but it is also relevant as the strategy indicates that only by increasing technological sovereignty, the goal of increasing the Union's cybersecurity could be achieved. Ultimately, the specific strategies presented to achieve technological sovereignty include building a more resilient infrastructure, the European Cyber shield, a reinforced presence on the technology supply chain, etc (Ibidem, 5-12).

Thematic and Narrative Analysis

Going into the thematic and narrative analysis, the presented strategy, similarly as others, contain provisions that don't have clear meaning. The results are presented in the table below.

Table 5.4 - A EU's Cybersecurity Strategy Thematic Analysis

Who or what is seen as the problem?	Digitalization	1
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Protectionist Measures	2

The first category is the most blurry one. The strategy refers to both digitalization and big tech as potential problems. However, Big Tech platforms occupy just a tiny space of the strategy as strategy only refers to them through an increasing market concentration (*The EU's Cybersecurity Strategy for the Digital Decade*, 2020, p. 2) or through reference to the EU's lower presence in technology supply chain (Ibidem, 11-12). On the other hand, digitalization occupies a central position in the strategy. Moreover, the COVID-19 pandemic is the event that further emphasized the importance of secured digital structure (Ibidem, 2-4).

Accordingly, the core orientation of the document is on the EU's security. Economic competitiveness is just briefly mentioned as an outcome of the further enhanced security on the EU and global level (Ibidem, 19-23). In the end, the strategy introduces numerous protectionist measures such as the joint cyber unit (p. 13), the EU cyber diplomacy toolbox (p. 16), and the improvement of cyber defense capabilities (p. 18). It should be noted that regulation is also reinforced but on a global level only through participation in numerous international bodies and multistakeholder frameworks (Ibidem, 20-23).

Total score: 5. The EU cybersecurity strategy contains almost complete security-oriented digital sovereignty discourse as the issues presented were more related

to the Union's security than economic competitiveness. The first dimension, in particular, lacked a stronger stance towards the Big Tech to achieve the score of 6.

Commission approves €5 billion German State aid measure to support ESMC in setting up a semiconductor manufacturing facility.

The presented communication represents a part of the series of the EC's approvals of state aid in case of crisis-relevant products (*Commission Approves €5 Billion German State Aid Measure to Support ESMC in Setting up a New Semiconductor Manufacturing Facility*, 2024, p. 2). Approving the state aid, the EC goes to justify the measure of the German state aid to construct a microchip manufacturing plant.

Identifying Digital Sovereignty Significance

The press release contains a significant digital sovereignty discourse. The critical aspect of the EU's strategy is the digital transition for which a resilient supply of microchips is essential (Ibidem, 2). Thus, the challenge recognized is clearly related to the digital sphere and, in particular, the semiconductor field. If the EU wants to achieve digital sovereignty then it needs to have a resilient flow of semiconductors outside of the established players in the industry from third countries.

The communication is relevant as the clear strategy for the achievement of digital sovereignty is laid down. Moreover, the concrete strategy is the approval of direct state aid to construction.

Thematic and Narrative Analysis

On the first glance, press releases like this seem to contain economic digital sovereignty discourse. However, the results present below indicate a different case.

Table 5.5 - A EC State Aid Approval to Germany Thematic Analysis

Who or what is seen as the problem?	Big Tech	2
What is the goal of digital sovereignty discourse?	Economic Competitiveness	1
What are the means proposed as the solution?	Protectionist Measures	2

Although Big Tech that are seen as a problem are direct beneficiaries of measures presented in the document, Big Tech producing microchips outside of the EU are seen as the problem. Thus, the measure presented is aimed at improving the EU's security in the semiconductor supply chain as microchips are essential for security in cyber spaces (Ibidem, 2). Ultimately, the measure is clearly protectionist as the EC's approval is only needed for measures that can distort competition.

Total score: 5. The measure presented will benefit the economic competitiveness of the EU but, the discourse of digital sovereignty presented is leaning towards security-oriented one. More precisely, measures are aimed to protect the EU's industry and security against the distortions caused by microchips shortages.

Digital Platforms as Regulated Entities: our Single Market, our rules.

In the annual conference of the EC Legal Service, the Commissioner for Internal Market and Services at the time, Thierry Breton, presented the core acts of the EU in digital spaces - Digital Markets Act (DMA) and Digital Services Act (DSA) (Breton, 2023a). Breton presented the acts as an immediate success as, from now on, "the EU has become the first jurisdiction in the world where online platforms no longer set their own rules" (Ibidem, 1). Moreover, Breton stressed that these acts "are an expression of European digital sovereignty" (Ibidem, 3).

Identifying Digital Sovereignty Significance

The speech delivered by Breton contains a significant digital sovereignty discourse. As Breton stated, DMA and DSA represent the expression of European digital sovereignty referring to the problem of platforms themselves regulating their operations (Ibidem, 1).

To express that the EU has digital sovereignty, the platforms must now comply with the new regulation if they want to do business in the single market.

Accordingly, digital sovereignty is the central theme in the speech as it refers to challenges in digital spaces while specifying the goal of achieving digital sovereignty. Moreover, the lack of regulation for online platforms is seen as a problem that is feasible to solve while the DMA and DSA are the rules that directly apply. Ultimately, Breton articulates digital sovereignty discourse not only by expressing the relevance of sovereignty in digital cases, but also its clear applicability through mentioned regulation.

Thematic and Narrative Analysis

In the depository, Breton's speech is named "Digital Platforms as Regulated Entities" thus clearly articulating the Big Tech as the main addressants of the speech. The rest of the analysis is presented below.

Table 5.6 - Digital Platforms as Regulated Entities Thematic Analysis

Who or what is seen as the problem?	Big Tech	2
What is the goal of digital sovereignty discourse?	Economic Competitiveness	1
What are the means proposed as the solution?	Standardization/Regulation	1

Big Tech companies own the biggest platforms used today. At the same time, these platforms are also gatekeepers serving as mediators between business and their customers (Breton, 2023a, pp. 1–2). These platforms set their own rules for operating thus negatively affecting safety, trustworthiness, and innovation on the internet. (Ibidem, 1).

Moreover, the goal of digital sovereignty discourse in the speech is to foster innovation, increase competitiveness and resilience. This will help companies "grow and expand in, and into, Europe, regardless of their geographic origin" (Ibidem, 2). Finally, the speech reinforces the obligation of online platforms and Big Tech owning them to comply with the EU rules if they want to operate on the EU market. The regulation also applies to

EU-based entities clearly showing that speech emphasizes regulation above protections measures as the solution.

Total score: 4. Breton's speech carries the significant economic-related discourse of digital sovereignty. Big Tech companies need to comply with the EU-adopted regulation if they want to operate within the single market so that everyone can thrive from improved competition and innovation (Ibidem, 1-3).

Statement at the European Parliament by President Ursula von der Leyen, candidate for a second mandate 2024-2029

On July 18th 2024, Ursula von der Leyen delivered her speech as the candidate for EC president for the second time. The analyzed speech represents the core of the EU action for the upcoming 5 years (Von der Leyen, 2024). In the period prior to the appointment of new EC, various legislative acts regulating digital spaces have been adopted including DMA, DSA, AI Act, EU Chips Act, and others. Surprisingly, the digital sovereignty discourse got very little attention in Von der Leyen's speech (Ibidem).

Identifying Digital Sovereignty Significance

Von der Leyen's speech doesn't include words sovereignty or autonomy in any instances. Although strong on the economic issues emphasizing the role of SMEs (Ibidem, 2) for the European ecosystem, the speech doesn't stress the importance of sovereignty in achieving greater economic competitiveness (Ibidem).

On one occasion, the speech mentions the importance of independent media that are often observed by digital giants (Ibidem, 4). On the other hand, Von der Leyen stresses that "from AI to clean tech, the future of our prosperity must be made in Europe" (Ibidem, 3).

Total score: Digital sovereignty discourse is not significant. The term digital sovereignty is not used in the speech. Moreover, only on a few occasions the speech indirectly refers to issues related with digital sovereignty. As all of the three criteria are missing, the document lacks digital sovereignty discourse.

Industrial sovereignty: we've come a long way (and it's only the beginning)

In another speech, Thierry Breton expanded on what he has previously said about digital entities to the comprehensive industrial strategy (Breton, 2023b). More precisely, the following speech focused solely on the critical dependencies treating Europe among the one in digital is essential (Ibidem, 1).

Identifying Digital Sovereignty Significance

Breton stresses the power of Europe that takes "industrial destiny into its own hands" (Ibidem, 1). Moreover, the Commissioner lays down three concrete strengths of Europe that would help it achieve industrial sovereignty: 1) the single market as a geopolitical tool, 2) ability to transform technological leadership into industrial and commercial, and 3) the strength of human capital (Ibidem, 1-4).

In all of these three and especially in the first one, digital sovereignty discourse has the central place. Breton states that "when Europe speaks, the big platforms listen" stressing the importance of rules adopted in the EU for its own market (Ibidem, 2). In other words, through the whole speech, the notion that the EU should be the one adopting rules in digital spaces is carried (Ibidem, 2-4).

Furthermore, critical dependencies existing in digital spaces as the main challenge can be and will be, according to Breton, solved by further regulating Big Tech, changing the state aid rules, improving regulatory and investment framework, etc. (Ibidem, 2-3). All of the actions are the elements of digital sovereignty where the EU, as a domestic authority, regulates, funds, and decides how digital solutions can be imported inside of the single market. In other words, steps are relevant and applicable making the digital sovereignty discourse significant.

Thematic and Narrative Analysis

As with the previous speech, Breton clearly identifies the problem being Big Tech companies. As he claims, the DSA and the DMA prevented Big Tech from using the mantra "too big to care" (Ibidem, 1). Moreover, Breton stresses that the EU's voice will be heard "from Brussels to San Francisco" (Ibidem, 1). Accordingly, Breton points out

to the Big Tech from the US as the problem. The same is applied to issues such as vaccines, semiconductors, advanced microchips, etc. by clearly labeling Big Tech companies as the problem. The rest of the results are presented in the table below.

Table 5.7 - The EU's Industrial Strategy Thematic Analysis

Who or what is seen as the problem?	Big Tech	2
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Protectionist Measures	2

In comparison to the previous speech, the current carries a stronger notion for state security as the whole EU industry is being observed, not just digital platforms (Breton, 2023b). Dependencies on semiconductors, digital platforms, energy, raw materials, etc. essential for digital are seen as the problem of security. The EU is not safe by being dependent on providers from third countries (Ibidem, 5).

Ultimately, throughout the whole speech, Breton emphasizes the protection of the EU from external shocks and shortages caused by dependence on external entities. Thus, the goal is to invest into domestic production, protect domestic industries and lay down a framework that favours European producers above external distorting competition.

Total score: 6. The speech by Breton contains a complete security-oriented digital sovereignty discourse. Stressed on many occasions in the speech, the EU was heavily impacted by the reliance on others which caused big insecurity in all fields. Thus, Europe must end being naive (Ibidem, 1) and enhance its security by being industrially and digitally sovereign.

Report on the state of the Digital Decade 2023

Based on the 2030 Digital Strategy previously assessed, the EC tracks the progress on how the current digital landscape is getting closer towards designated goals. The report stresses key challenges so far and urges the member states to step up their efforts towards digital transformation (European Commission, 2023).

Identifying Digital Sovereignty Significance

The 2023 report on digital decade goals contains a significant digital sovereignty discourse as it fulfills all three criteria. More precisely, the document discusses problems and challenges related to digital sovereignty in numerous instances. In the first place, the document stresses critical dependencies of the EU in digital space as the EU's share of the global ICT revenue is falling while the US one is growing (Ibidem, 7). Moreover, 80% of digital products or services used in the EU market are being provided by the external companies making the EU vulnerable. Special emphasis is placed on the 5G network development in the EU urging member states to ensure digital sovereignty and secure supply in this market (Ibidem, 13).

Secondly, the document presents specific proposals to address the digital sovereignty challenges such as the EU Chips Act, 5G Toolbox Implementation, and others that underline the relevance of the digital sovereignty discourse (Ibidem, 13-14). Finally, these solutions are not only relevant but also applicable as many frameworks mentioned in the document are adopted to boost investment and foster the creation of the EU-based solutions over external ones (Ibidem, 19-20).

Thematic and Narrative Analysis

The report identifies foreign Big Tech companies as a major challenge to the EU's digital sovereignty. These companies are seen as the main beneficiaries of the EU's dependencies in fields such as cloud computing, AI, semiconductors, and data services. Moreover, the report stresses the problem of market concentration of a few large companies that limits the EU's capabilities of developing sovereign digital infrastructures (European Commission, 2023, pp. 11–17).

Critical dependencies mentioned are in favour of the EU's security as the intensified geopolitical situation stresses the importance of having a resilient supply chain and protection against cybersecurity threats (Ibidem, 7).

Table 5.8 - The 2023 Digital Decade Report Thematic Analysis

Who or what is seen as the problem?	Big Tech	2
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Standardization/Regulation	1

In the end, the means of achieving EU's security is predominantly presented through adoption of broader regulation. The report pushes for the more ambitious implementation of the crucial regulation in the EU in the digital sphere such as DSA, EU Chips Act, Cyber Resilience Act, and others.

Total score: 5. The report emphasizes EU's security over economic competitiveness as the global polarization grows. Enhanced geopolitical competition between the US and China urges the EU to develop domestic capabilities in some of the crucial sectors such as AI, semiconductor, quantum computing, and others. Thus, the main orientation of the discourse presented is the EU's resilience and security against external threats.

EU Strategic Dependencies and Capacities: Second Stage of In-Depth Interviews

The presented report contains analysis of the five areas: rare earths and magnesium, chemicals, solar panels, cybersecurity, and IT software where the EU is dependent on providers from third countries (European Commission, 2022). Particularly areas of cybersecurity and IT software are at core of the EU's digital sovereignty strategy and its transition to a digital, resilient, and competitive economy (Ibidem).

Identifying Digital Sovereignty Significance

The presented report discusses strategic dependencies in the digital sector, emphasizing the amount of products and services the EU depends on. Among others, the key challenges related to digital sovereignty are cloud computing and AI technologies development (Ibidem, 61-68).

More specifically, the report states that the EU currently lacks alternatives to leading cloud providers such as Microsoft, Amazon Web Services (AWS), and Google Cloud that are holding the majority of the market share. At the same time, the report urges EU countries to focus on investments that would reduce these dependencies and achieve EU's digital sovereignty (Ibidem, 69). Thus, the idea that the EU must be digitally sovereign contains a central position in this document as challenges related to the EU-based rules on the EU market are making up the largest portion of the document.

Ultimately, documents outline further stress the importance of digital policies already adopted in the EU, such as DMA, DSA, Data Act, and others that are aimed at reducing these dependencies and achieving sovereignty in digital spaces. In those spaces, the EU is already applying strategies such as Next-Generation Cloud Infrastructure, the EU alliance for industrial Data, Edge, and Cloud, and many others (Ibidem). Consequently, challenges in the document related to digital sovereignty are central, strategies mentioned are relevant and applicable to solve them. Digital sovereignty discourse presented is significant.

Thematic and Narrative Analysis

The report specifically mentions the US-based tech giants such as Google, Amazon, and Microsoft as leaders in cloud computing that are seen as the biggest problem due to their market dominance and the EU's dependence on them in cloud computing (European Commission, 2022, pp. 61–62).

Table 5.9 - The EU Strategic Dependencies and Capacities Thematic Analysis

Who or what is seen as the problem?	Big Tech	2
What is the goal of digital sovereignty discourse?	Economic Competitiveness	1
What are the means proposed as the solution?	Standardization/Regulation	1

Moreover, the document puts emphasis on competitiveness as the major US corporations are mentioned only to stress the market dominance. The European market, on the contrary, should foster fair competition without concentration of market power

within few players (Ibidem, 69). In particular, the EU-based companies should have a free choice on which cloud service they will subscribe to store their data (Ibidem, 70). Ultimately, the document mentions and carries the logic of some of the most important regulations of the EU such as DMA, DSA, EU Edge and EU Cloud computing regulation (Ibidem, 67-68). Although the document refers to a couple of selective protectionist measures, standardization and regulation through fair competition laws occupy the major part.

Total score: 4. The economic digital sovereignty discourse prevails over a security-oriented one in this document because the primary focus is on enhancing Europe's industrial competitiveness and reducing reliance on non-EU digital infrastructure. While state security considerations are acknowledged the document frames them within an economic context, aiming to secure supply chains and protect European industries from external dependencies.

5.2. The Digital Sovereignty in the EU - Recap

The analysis of EU documents on digital sovereignty reveals a nuanced approach. Out of eleven documents analyzed, our analysis found a significant digital sovereignty discourse in nine of them. Four documents primarily focus on digital sovereignty as a means to enhance economic competitiveness. These emphasize fostering innovation, investment, and reducing dependence on non-EU tech providers while ensuring a fair digital market. European Strategy for Data is the only document receiving a score of 3 indicating a clear economically-oriented digital sovereignty discourse.

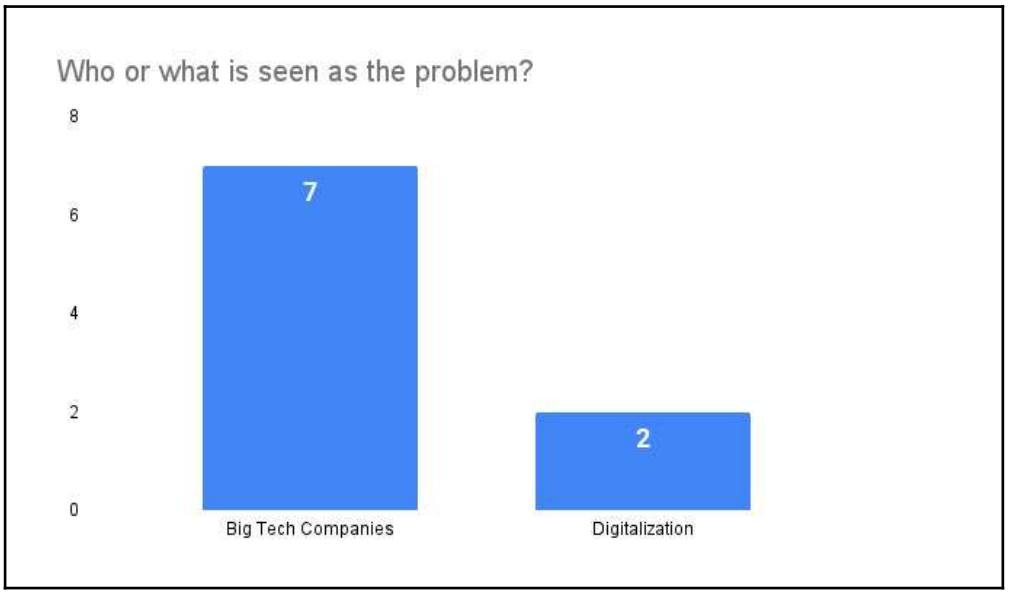
On the contrary, five documents frame digital sovereignty primarily in security terms, focusing on protecting digital infrastructure, cybersecurity, and resilience against foreign dependencies. The speech on Industrial Sovereignty by Breton is the only document receiving a score of 6 indicating a clear security-oriented digital sovereignty discourse.

Table 5.10 - Total Results

Economically-oriented Digital Sovereignty Discourse	4
Security-oriented Digital Sovereignty Discourse	5
Without significant Digital Sovereignty Discourse	2

Going through question-by-question analysis, it can be argued that the EU perceives Big Tech companies as the main problem in the digital sphere as 7 of the 9 documents recognized Big Tech as the main challenge.

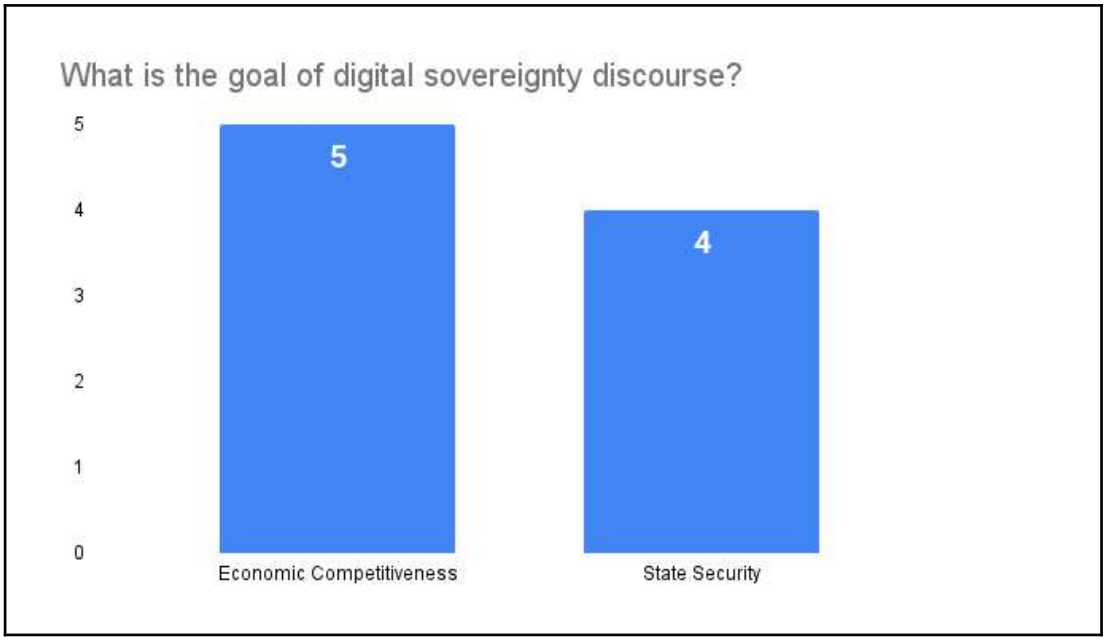
Table 5.11 - Breakdown of responses to First Question



US-based tech giants such as Amazon, Microsoft, Google, and Apple are seen as the biggest obstacle towards the achievement of digital sovereignty by the EU as they hold a large share of the market. Until recently, these actors relied on self-regulation which further impeded EU's sovereignty in digital space.

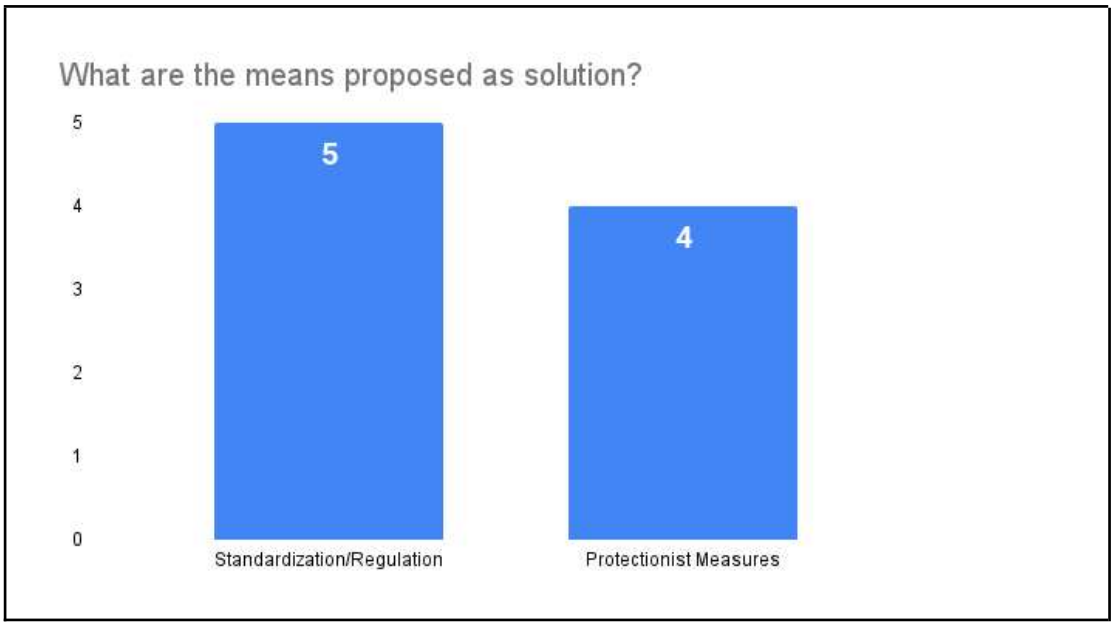
The breakdown of question two shows less distinctive results as neither side prevailed dominantly. Although economic competitiveness prevailed, security-related issues present in all of them as documents carried the strong narrative of building a secure and resilient single market to external threats. In connection with the majority of answers of the first question, it is clear that the EU sees Big Tech companies both as a threat to its economic competitiveness as well as security.

Table 5.12 - Breakdown of responses to Second Question



Last but not least, the analysis of responses to the final question shows that the EU slightly favours standardization and regulation over protectionist measures as the former was present in 5 and the latter in 4 documents. This finding reflects the EU's dual strategy in digital sovereignty: the EU promotes standardization and regulatory frameworks to create a unified digital market and enhance technological governance. On the other hand, it implements protectionist measures aimed at reducing dependency on foreign digital infrastructure and reinforcing its strategic autonomy.

Table 5.13 - Breakdown of responses to Third Question



The analysis of digital sovereignty in the EU reveals the balance existing between economic competitiveness and state security. The EU conceptualizes digital sovereignty as a dual strategy that incorporates economic and security concerns. The main drive of the EU in digital spaces is to adopt policy measures that would limit the power of Big Tech companies that are perceived as a major obstacle to sovereignty (*A European Strategy for Data*, 2020). Operationally, the EU favors standardization and regulation where digital sovereignty is pursued through market rules, digital governance, and industrial policy rather than direct protectionist measures.

Moreover, the EU's sovereignty claims represent the combination of regulation and strategic autonomy characterized by:

- Regulatory and legal frameworks as the primary tool for the exertion of sovereignty.
- Rule-based approach that aligns digital sovereignty with democratic values.
- A dual narrative that balances innovation with resilience.

In the end, the EU's digital sovereignty strategy is neither purely protectionist nor entirely open-market-driven. Instead, it operates within a hybrid model, leveraging standardization and regulation to maintain a competitive yet controlled digital space.

5.3. Digital Sovereignty of India Documents Analysis

National Strategy for Artificial Intelligence (AI)

In 2018 NITI Ayaog, an essential public policy think tank of India published the National Strategy for AI. NITI Ayaog serves the government of India as the body that drafts essential documents to catalyze economic growth. The document carries the message of using AI for inclusive growth and positioning India as the leader in the AI ecosystem (NITI Ayog, 2018a, p. 5). Labelled as the essential document for AI development India, the strategy covers applications in various sectors such as mobility, healthcare, agriculture, education, and others. (Ibidem).

Identifying Digital Sovereignty Significance

When criteria of digital sovereignty discourse are applied to this document, somewhat blurred results are obtained. In the first place, the document does not specifically mention digital sovereignty or related terms. Moreover, the document discusses concepts closely related to digital sovereignty such as data governance, privacy, AI governance, etc (Ibidem, 55-65). Also issues such as data security and ethics in obtaining data are mentioned but without specific reference to digital sovereignty.

Across the whole document, the digital sovereignty frame takes little to no space. Issues that are mentioned are only there because the policymaker recognized weakness of India in that sphere that needs to be addressed by increasing investment, financing universities, and exchange of knowledge (Ibidem, 71-74). None of these is framed as a sovereignty but rather a development issue. Compatible document of the EU, the AI act contains strong provisions about third-country providers that are doing business in the EU and the necessity to regulate them (*EU AI Act*, 2023, p. 6).

Accordingly, the centrality criteria is not fulfilled. Regarding other two criteria, only partial solutions are proposed and they are framed as economic enablers rather than protectors of digital sovereignty of India. Ultimately, the strategy mentions investments into the AIRAWAT structure as a domestic hub for AI development that would prevent dependencies on external actors (NITI Ayog, 2018a, p. 59).

Total score: Digital sovereignty discourse is not significant. Although the strategy mentions foreign AI infrastructure that India is somewhat dependent on, the document is predominantly focused on improving the economic and R&D capabilities of India to catch up with the AI revolution rather than achieve greater sovereignty.

Digital India Act

The Digital India Act represents one of the newest pieces of legislation in India that is still in the process of adoption but the core materials are available to the public (Chin, 2024). The act was adopted to replace the active Technology (IT) Act that was adopted in 2000 and labelled obsolete by many observers (Ibidem). According to the Ministry of Electronics and Information Technology, the goal of the new act will be to allow more innovation for the Indian economy while preserving the safety of online spaces (Ibidem).

Identifying Digital Sovereignty Significance

The available material on the Act suggests the presence of significant digital sovereignty discourse. Regarding centrality, while it does not explicitly use "digital sovereignty," the underlying themes of regulatory independence, control over data, and AI governance are evident. In particular, the Act seeks to regulate Big Tech and govern emerging technologies to ensure that India remains an independent and trusted digital economy (Ministry of Electronics and IT, 2023).

Moreover the Act strongly emphasizes the misconduct done by big companies such as Meta, Netflix, Google, and others calling for stronger market competition rules and safer environment for Indian start-ups (Ibidem, 16). Other than Big Tech, the Act also proposes relevant strategies for Data Protection, AI regulation, and National Digital Infrastructure (Ibidem, 17-21).

Ultimately, The Act provides concrete implementation steps to strengthen India's digital sovereignty through a legislative and enforcement framework. It also promotes the "whole-of-government" approach calling for a unified approach in all of the mentioned fields (Ibidem).

Overall, the Act is highly applicable as it outlines specific regulatory actions, but some areas still require clarity on enforcement mechanisms as the Act is still in the adoption phase.

Thematic and Narrative Analysis

The Act addresses critical challenges to India's digital sovereignty, focusing on the dominance of Big Tech and the lack of accountability in their practices. It identifies tech platforms as a major concern, particularly their control over algorithms, data, and markets (Ministry of Electronics and IT, 2023).

Table 5.14 - The Digital India Act Thematic Analysis

Who or what is seen as the problem?	Big Tech	2
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Standardization/Regulation	1

The Act's goal is to improve state security by protecting India's cyberspace, ensuring robust privacy safeguards, and mitigating risks posed by emerging technologies like AI and surveillance devices. However, there is a clear overlap with competitiveness discourse as the trustworthy digital space also indirectly focuses on economic aspects (Ibidem). In the end, the Acr proposes a robust legislative framework to ensure AI accountability, data protection, intermediary governance, and cybersecurity resilience. These measures prioritize creating a secure, open, and trusted internet ecosystem, while balancing innovation with regulation (Ibidem).

Total score: 5. While elements of economic competitiveness are addressed, the Act primarily emphasizes the protection of India's digital infrastructure and ensuring control over emerging technological risks stemming primarily from Big Tech. However, these threats are also seen from the ability of start-ups to innovate so the security-oriented digital sovereignty discourse is not complete but contains some part of the economic one, namely in regulation.

The Digital Personal Data Protection Bill

The Digital Personal Data Protection Bill was introduced in 2023 to regulate the management of personal data in India. Initially, the conversation about the new Bill in India that deals with personal data started back in 2017 as a response to the newly adopted GDPR in the EU (Tejasi Panjiar & Radhika Roy, 2023). The bill was designed to replace earlier drafts of the Personal Data Protection Bill, 2019, which faced criticism for its complexity and lack of alignment with modern data protection norms (Ibidem).

Identifying Digital Sovereignty Significance

The Bill introduces the rules around data control, privacy, and security while also stressing how both domestic and international actors must handle personal data (DPD Bill, 2023). The Bill doesn't specifically mention the notion of digital sovereignty but it includes strong provisions that aim to establish a strong governance framework for handling data inside of India and by the Indian government (Ibidem). Moreover, the Bill regulates Big Tech as Significant Data Fiduciaries (SDFs) as entities having a big impact in data management (Ibidem, 9). Similarly as the European Strategy for Data, all entities marked as SDF must have a data officer in India (Ibidem, 9). Thus digital sovereignty discourse is central for this document.

Relevance and applicability criteria are fulfilled through the provisions established about the Data Protection Board of India. These provisions clearly see the misconduct of personal data and digital sovereignty as relevant problems so the concrete strategies are laid down (Ibidem). The particularly important one is about the SDFs that will be subject to the special regime as they usually handle a vast amount of personal data and are located outside of India (Ibidem). Thus, the bill contains a significant digital sovereignty discourse.

Thematic and Narrative Analysis

The Bill implicitly identifies Big Tech and large data fiduciaries as key entities requiring regulation. By classifying some companies as SDFs, the Bill highlights concerns about the unregulated processing of Indian user data, lack of transparency, and the influence of foreign tech giants. Moreover, strong provisions regarding cross-border data transfers

highlight the orientation of the document towards Big Tech companies as these have the biggest impact on the sovereignty of the state (Ibidem).

Table 5.15 - The Digital Personal Data Protection Bill Thematic Analysis

Who or what is seen as the problem?	Big Tech	2
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Standardization/Regulation	1

Regarding the second question, the nill's primary objective is to ensure India's control over its digital ecosystem, particularly in how personal data is collected, processed, and transferred. The creation of the Data Protection Board of India reflects a move toward centralized oversight of data governance, reducing foreign influence in India's digital infrastructure. Finally, the bill proceeds with the regulation as the means to improve the state's security. As mentioned earlier, entities handling large amounts of data are obliged to comply with the set of rules ensuring legal oversight of both domestic and foreign data handlers (Ibidem).

Total score: 5. The score of the Bill indicates a predominant orientation towards security-based digital sovereignty discourse with a few economic competitiveness considerations. However, its core focus remains on state control over data governance and limiting foreign influence.

The Strategy for New India @ 75

The strategy for New India @75 represents a comprehensive document adopted at the end of 2018 that serves as the plan for the Indian government for development up to 2022, which marks the 75th anniversary of Indian independence (NITI Ayog, 2018b). The document outlines 41 key areas of policy focus, aiming to drive sustained economic growth and digital transformation.

Identifying Digital Sovereignty Significance

The presented strategy touches on several issues that are connected to digital sovereignty such as cyber security and localized digital ecosystems but the document does not adopt a digital sovereignty framework. The focus of the document is digital transformation and the overall enhancement of the digital economy (Ibidem). Accordingly, the discourse of digital sovereignty in the document is very weak while strategies presented are not relevant or applicable while the central goal is not connected with the sovereign control of national infrastructure or any other similar issues such in other documents analyzed.

Total score: Digital sovereignty discourse is not significant.

The National Digital Communication Policy

The NDCP was launched by the government in India in 2018 aiming to secure safe and secure digital infrastructure for economic development (Ministry of Communications, 2018). The goal of the policy was also to improve connectivity of remote areas in India that are lacking essential infrastructure for communication.

Identifying Digital Sovereignty Significance

The policy lays down a few missions to be achieved in the first 4 years of. One of the missions discussed is “Secure India” (Ibidem, 5) stressing the importance of digital sovereignty in achieving so. The document stresses the importance of Indian entities having a free choice to select the best possible services along with the ownership of communication infrastructure (Ibidem, 5-6). Overall, the document presents challenges related to digital infrastructure and lays down concrete strategies for solving them.

Regarding the relevance criteria, the policy focuses on the promotion of domestic innovation, localized cybersecurity, and robust data protection laws are strong indicators that this policy aligns with digital sovereignty goals (Ibidem). Ultimately, the NDCP gives concrete steps and strategy for achieving digital sovereignty through the establishment of a strong Data Protection regime (p. 18), providing autonomy for every citizen (p. 18), and secure digital infrastructure (p. 19).

Thematic and Narrative Analysis

The document identifies the problem of digital infrastructure that is currently lacking in most of the remote parts of India. Accordingly, the main problem seen by the document is digitalization and issues caused by it if the proper infrastructure is not developed (Ministry of Communications, 2018).

Table 5.16 - The NDCP Thematic Analysis

Who or what is seen as the problem?	Digitalization	1
What is the goal of digital sovereignty discourse?	Economic Competitiveness	1
What are the means proposed as the solution?	Standardization/Regulation	1

The digital sovereignty discourse presented is completely in the favour of economic competitiveness of India. The document stresses the importance of domestic capacities to reach the fast pace of digitalization and increase the chances of India to compete in the connected world (Ibidem, 1-2). On the other hand, although protectionist measures are mentioned in the document, the inclusion of standards and regulation is what the discourse focuses on. In other words, the focus of the document are regulatory frameworks and harmonized policies to ensure efficient digital governance (Ibidem).

Total score: 3. The NDCP presents a digital sovereignty discourse that is primarily economically-oriented, with a focus on addressing digitization challenges and India's chance to benefit from it economically. To do that, India needs to improve its communication infrastructure and improve its position in the global value chain.

Speech of Prime Minister Narendra Modi at the 18th Asia-Pacific Conference of German Businesses (APK) 2024

The presented speech was made by the Indian Prime Minister, Narendra Modi, that was organized between India and Germany aimed at strengthening their bilateral ties and fostering cooperation. Among other things, Modi focuses on India's commitment to creating a business-friendly environment through regulatory reforms, infrastructure development, and innovation (Modi, 2024a). The speech reflected India's ambitions to

strengthen bilateral relations and invites German businesses to take advantage of the vast opportunities within India's dynamic market.

Identifying Digital Sovereignty Significance

Modi's speech at the German-Indian conference doesn't contain a significant digital sovereignty discourse. On the contrary, the speech primarily focuses on economic growth, investment opportunities, and India's digital transformation, rather than digital sovereignty. While he highlights initiatives like Mission AI, the Semiconductor Mission, and the Digital India Mission, these are framed as opportunities for global collaboration rather than national control over digital infrastructure (Ibidem).

The speech lacks explicit references to data localization, cybersecurity governance, or restrictions on foreign technology firms, indicating that digital sovereignty is not a central theme. Thus the criteria of centrality, relevance, and applicability are not fulfilled.

Total score: Digital sovereignty discourse is not significant.

PM delivers keynote address at The Sydney Dialogue, speaks on India's technology evolution and revolution

At an annual summit organized by the Australian Strategic Policy Institute (ASPI) focusing on critical, emerging, and cyber technologies, the prime minister Modi delivered a speech around Indian position in these technologies. He also discussed the importance of international collaboration in addressing the challenges posed by rapid technological changes (Modi, 2021).

Identifying Digital Sovereignty Significance

Prime Minister Narendra Modi's keynote address at *The Sydney Dialogue* contains significant discourse on digital sovereignty, particularly in the context of India's evolving role in the digital age. The speech meets the centrality criterion, as it identifies key challenges related to digital sovereignty, including cybersecurity threats, data privacy concerns, responsible AI governance, and the risks associated with crypto-currency misuse (Ibidem). Modi underscores the need for secure and resilient digital infrastructure while warning against the misuse of democratic openness by

vested interests. His emphasis on the intersection of democracy, technology, and security places digital sovereignty at the core of his address advocating for the bigger role of the Indian government (Ibidem).

The speech also fulfils the criteria of relevance as it proposes concrete measures to address these challenges. Modi highlights India's push for indigenous technological capabilities in 5G, 6G, AI, and semiconductor manufacturing, ensuring greater digital self-reliance.

However, while the speech outlines several broad strategies, it only partially meets the applicability criterion, as it lacks specific policy implementation details (Ibidem). Since the presented document is the speech, the lack of specific policy implementation is expected as these types of steps are usually located in written policy documents and strategies. Accordingly, this Modi's speech contains a significant digital sovereignty discourse.

Thematic and Narrative Analysis

Modi does not position digitalization itself as the problem but rather focuses on how digital openness can be misused by interests of large players in the industry (Modi, 2021). He highlights cybersecurity threats, the manipulation of public opinion, concerns over crypto misuse, and the need for secure data governance, which allude to the role of large tech platforms and global digital actors in shaping digital risks.

Table 5.17 - The NDCP Thematic Analysis

Who or what is seen as the problem?	Big Tech Companies	2
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Protectionist Measures	2

While Modi discusses digital competitiveness through India's startup ecosystem and AI leadership, the primary focus is on national security. He stresses the need to secure India's digital infrastructure, prevent cyber threats, ensure data privacy, and maintain democratic integrity (Ibidem). His call for international cooperation in cybersecurity

and regulation of digital assets reinforces the notion that digital sovereignty is framed as a national security priority rather than purely an economic competitiveness issue (Ibidem).

Modi's speech highlights domestic capacity-building and self-reliance in digital technologies. His mention of incentives for semiconductor production, indigenous 5G and 6G development, and investment in local tech manufacturing indicates a protectionist approach aimed at reducing dependence on external technology providers. While standardization and regulation are discussed, the dominant theme is enhancing national technological autonomy, aligning more with protectionist measures (Ibidem).

Total score: 6. Consequently, the speech contains the digital sovereignty discourse that is purely security-oriented. The speech frames digital sovereignty primarily as a national security issue, positioning Big Tech and external digital dependencies as key concerns. While economic competitiveness is mentioned, security remains the dominant narrative.

Today, India is the world's fastest-growing large economy, attracting global partnerships: PM

This speech was delivered by the Indian PM, Narendra Modi, on the News9 Global Summit in Stuttgart, Germany, on the occasion of the 25th anniversary of the German-Indian strategic partnership (Modi, 2024b). The topics covered in the speech were the economic growth of India and the growing opportunities for German companies to invest in it, technology and innovation in India with focus on some essential technologies such as semiconductors, and etc (Ibidem).

Identifying Digital Sovereignty Significance

Going through the digital sovereignty discourse criteria, this speech by Modi does not meet them. To begin with, the goal of the speech is to present the technological and policy reforms in India that could make the potential investments from Germany easier (Ibidem). Moreover, the speech does not present challenges related to the digital sphere in which the increase of jurisdiction and sovereignty would pose as the solution. Although some digital challenges are presented, they are not related to digital sovereignty issues.

Regarding the other two criteria, the speech does not mention any clear steps, frameworks, or policies directly aimed at solving digital sovereignty-related issues. Furthermore, the control of national digital assets usually addressed in speeches with significant digital sovereignty discourse is missing from this speech (Ibidem). Accordingly, applicability and relevance criteria are not fulfilled.

Total score: Digital sovereignty discourse is not significant. While the speech discusses technological growth and digital infrastructure, it lacks explicit mention of digital sovereignty, its challenges or actionable strategies.

Today India is working in every sector, in every area with unprecedented speed: PM at NDTV World Summit

This speech by Modi was delivered in October, 2024 at the NDTV World summit (Modi, 2024c). The main topics covered by the speech were the growth of India and digital infrastructure that allow the possibility of foreign investment in the country. On the other hand, the main goal was to position India as a key player in global discussions on technology, AI, and climate change.

Identifying Digital Sovereignty Significance

Regarding the digital sovereignty discourse criteria, the speech presented fulfils the three criteria, but only partially. In the first place, the document mentions several infrastructural projects that are related to digital sovereignty-related issues such as digital public infrastructure (DPI), UPI, Aadhaar, and OND (Ibidem) but none of these is clearly mentioned in the context of control of digital assets or other seen issues connected to digital sovereignty.

Moreover, The speech highlights India's digital infrastructure advancements but does not offer specific solutions for digital sovereignty issues. The closest thing that the speech contains about digital sovereignty is the mentioning of “democratized technology” rather than monopolization present in other countries (Ibidem). Ultimately, the references in the speech are predominantly focused on India’s digital progress, not strategies for improvement of sovereignty in digital spaces.

Total score: Digital sovereignty discourse is not significant. In conclusion, the speech is more about economic growth and India's global role, rather than governance of essential technologies or national control over digital assets.

Annual Report (Digital Governance) Ministry of Electronics and Information Technology

The presented report outlines the current progress of Digitalization in India covering a range of topics including strategy for crucial technologies, IT, cyber security, cloud infrastructure and many others (Ministry of Electronics and Information Technology, Government of India, 2024). Moreover, the report represents an essential document for the government's action in policy planning of crucial technologies and international cooperation (Ibidem). Thus, the document covers various aspects of the digital sovereignty discourse.

Identifying Digital Sovereignty Significance

When run to the three criteria presented, the report contains a significant digital sovereignty discourse. In the first place, at its core the report contains challenges connected to digital sovereignty such as cyber security, AI, and cloud infrastructure. All of these challenges are presented in the light of the Indian government having control over the digital assets. The IndiaAI mission is mentioned as the way of democratising the control over AI and, more importantly, ensuring that national data stays within Indian control (Ibidem, 14-15; 160-170). Moreover, the MeghRaj Cloud Initiative (GI Cloud) mentioned refers to the control of cloud infrastructure by Indian companies (Ibidem, 25-27). Consequently, these issues occupy the central place in the document while also being referred to in terms of sovereign control.

Not only does the report mention these challenges, but it also stresses relevant and applicable strategies to solve digital sovereignty-oriented issues. Some of the strategies highly relevant that are mentioned are the India Semiconductor Mission (ISM) and Production Linked Incentive (PLI) that aim to boost domestic production of semiconductors and reduce the dependence on foreign suppliers (Ibidem, 123-151). At the same time, documents such as the Digital personal data protection act are mentioned in the light of setting strict rules on data processing of Indian citizens (Ibidem, 14; 147).

Thematic and Narrative Analysis

The challenges presented in the document that are digitally-related (AI, cyber security, cloud infrastructure, and etc.) are mentioned referring to big tech companies that are causing strategic dependencies in those fields. Data protection act, MeghRaj cloud initiative, or IndiaAI mission are discussed from the perspective of big tech companies dominating in their respective fields (Ibidem, 14-16; 25-27). Most of these companies referred to are foreign so the discourse clearly sees big tech companies as the main challenge.

Table 5.18 - The Digital India Annual Report 2023-24 Thematic Analysis

Who or what is seen as the problem?	Big Tech Companies	2
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Protectionist Measures	2

To continue, Big Tech companies are seen to harm the security of India and its companies thus stressing the state security of being the ultimate goal. Two overarching goals of the report are to secure the digital infrastructure of India from foreign threats (Ibidem, 256) and to reduce reliance on foreign tech (Ibidem, 22-26). The language used in both of the goals is to ensure that business and data of Indian citizens and companies is protected.

Ultimately, the report advocates for measures that are protecting Indian companies, mainly, from external competition. These measures are a MeghRaj initiative allowing Indian businesses to store their data on Indian-managed cloud storage (Ibidem, 25-27), to foster domestic industries by protecting them from foreign competition in semiconductor production and AI-systems development (Ibidem, 151; 160).

Total score: 6. The report discussed presents the issue of digital sovereignty in security-related terms. It stresses the national control over critical infrastructures for the sake of protection, namely from Big Tech companies that are dominant in the field.

Critical Minerals For India Report

The critical minerals report is the report adopted by the Ministry of Mines in 2023 and represents the document that provides a comprehensive assessment of minerals essential for India's economic growth, energy transition, and national security (Ministry of Mines, Government of India, 2023). Moreover, the report highlights supply chain vulnerabilities, import dependencies, and strategic measures to ensure India's self-sufficiency in critical minerals that are essential for the country's ambition in digital technology development (Ibidem).

Identifying Digital Sovereignty Significance

Going through the criteria, the report identifies areas that are problematic due to the strategic dependencies for minerals such as Gallium, Germanium, Indium, and Silicon. These minerals are essential for technologies such as semiconductors and electronics (Ibidem, 22; 35-37). The report stresses the dependence on suppliers from China, Russia, and the US putting the idea of producing critical minerals on the Indian territory. Thus, the document contains a central digital sovereignty discourse.

Regarding the other two criteria, the report lays down strategies that are relevant and applicable for solving these strategic shortages. In particular, it stresses measures such as domestic resource development (Ibidem, 37), supply chain diversification (Ibidem, 25), and self-reliance in critical mineral processing (Ibidem, 30-33). All of these indicate that the report contains the significant digital sovereignty discourse.

Thematic and Narrative Analysis

The report sees digitization as the opportunity for the development of India. However, the essential minerals required to do so are lacking thus positioning dependence on foreign companies as the key problem. Although companies seen as the problem are not Big tech companies in the strict meaning of the word, dependencies on foreign minerals and network of companies operating them are understood as the key issue (Ibidem).

Table 5.19 - The Digital India Annual Report 2023-24 Thematic Analysis

Who or what is seen as the problem?	Big Tech Companies	2
What is the goal of digital sovereignty discourse?	State Security	2
What are the means proposed as the solution?	Protectionist Measures	2

The report mentions that India is currently 100% dependent on imports of some materials (Ibidem, 4). Accordingly, these shortages are seen as the threat to national security as India cannot count on domestic production of these materials that are inputs in critical infrastructure such as clouds, AI, and certain sectors of the defense industry. Without them, the report argues, core functions of the Indian state could be hindered such as the defense and safe structure of the digital economy and payments (Ibidem). Ultimately, the only way to reduce the dependencies presented in the report is to protect the domestic production and ramp up the measures of importing external materials (Ibidem).

Total score: 6. The report presents digital sovereignty as a matter of national security, not just economic competitiveness. It strongly advocates for state intervention and protectionist policies to secure critical minerals, which are foundational to some of key issues such as AI, cybersecurity, and digital infrastructure.

5.4. The Digital Sovereignty in India - Recap

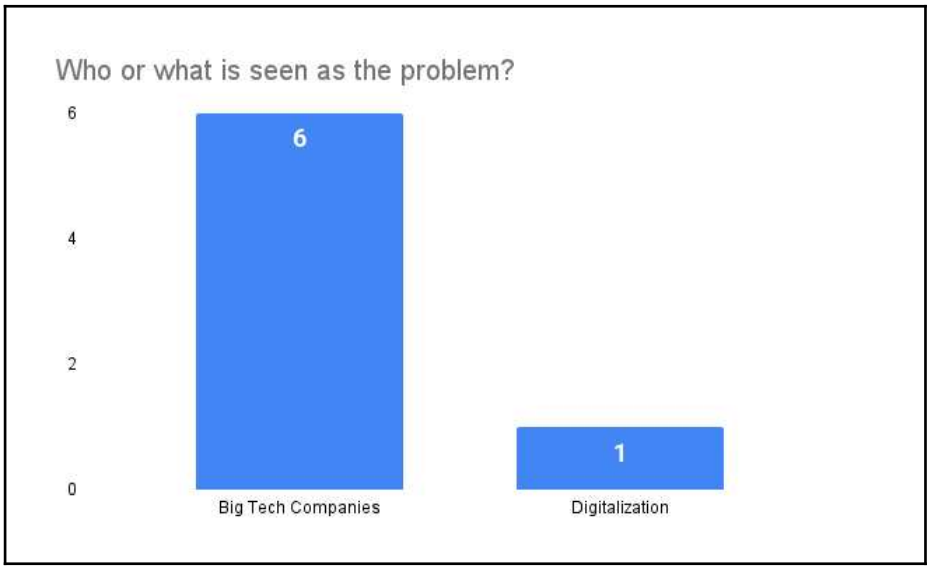
The digital sovereignty discourse analysis of eleven Indian documents discovered the significant discourse in six of them, three less than the EU analysis. Compared to much more nuanced results of the EU digital sovereignty, Indian documents were predominantly security oriented, framing digital sovereignty-related issues as national security threats and advocating for protectionist measures. More precisely, the only document from the Indian side, National Digital Communication Policy (NCDP), had an economically-oriented digital sovereignty discourse.

Table 5.20 - Total Results

Economically-oriented Digital Sovereignty Discourse	1
Security-oriented Digital Sovereignty Discourse	6
Without significant Digital Sovereignty Discourse	4

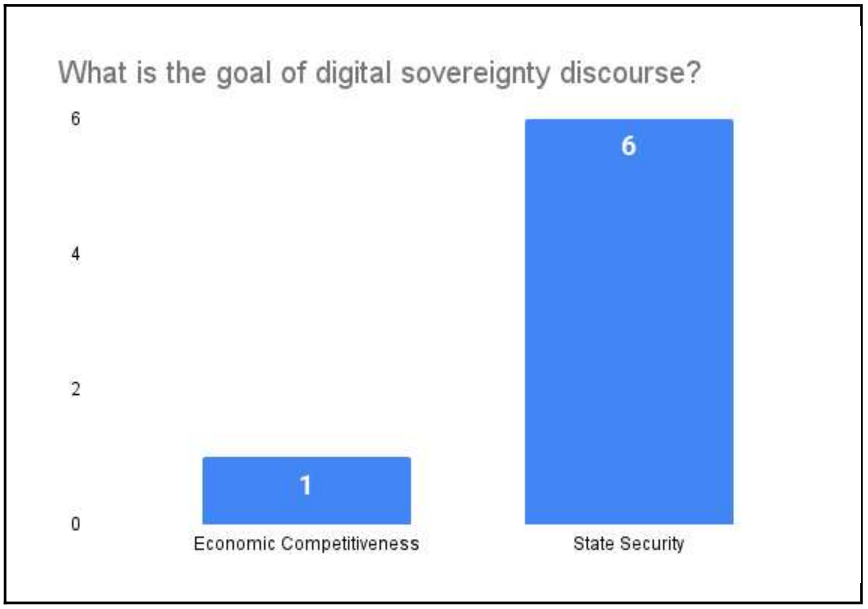
The analysis of responses to three essential questions show the following results. In the first place, Indian policy-makers see the Big Tech and foreign-controlled supply chains as the dominant concerns. More precisely, only one (Ministry of Communications, 2018) out of six documents saw digitalization as the crucial problem while the remaining five saw the dominance of Big Tech as the crucial issue.

Table 5.21 - Breakdown of responses to the first question



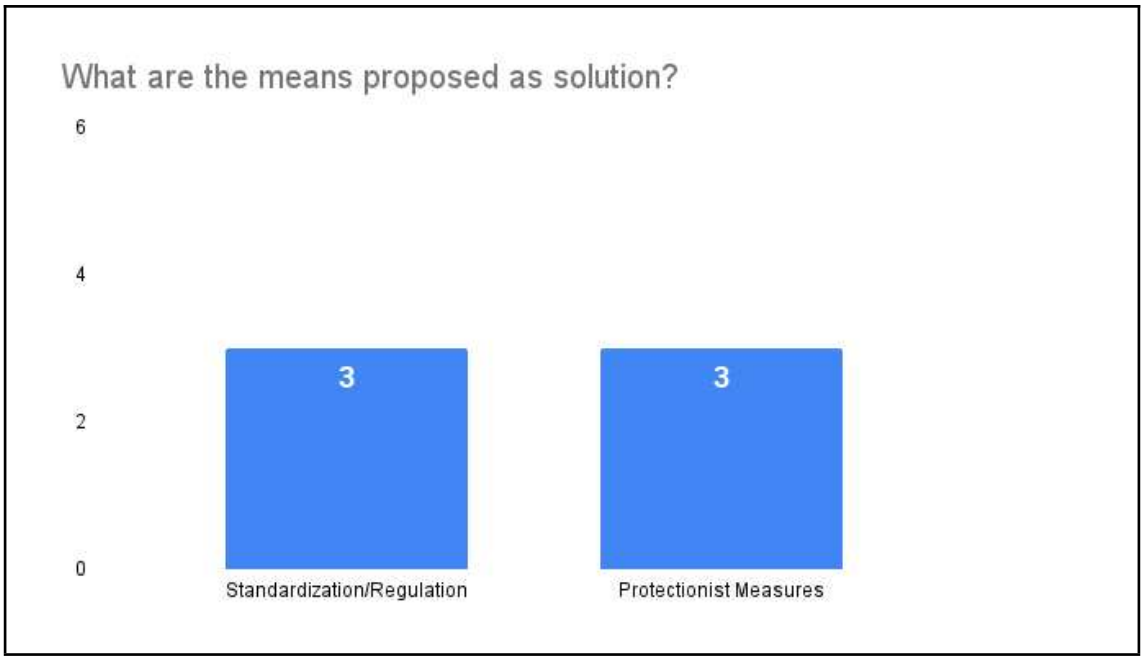
Although the view of digital sovereignty in India varies across policy domains, the dominant notion present is national security. In other words, the dominant conceptualization in all the policy domains is the security one showcased by the documents in which five out of six of them showcased security rather than economic orientation.

Table 5.22 - Breakdown of responses to the second question



In the end, the responses to the third question were evenly distributed as three documents were focused dominantly on protectionist measures and three on introduction of standards and regulations. Interestingly, although India sees Big Tech and security-issues as the most relevant, the means of achieving the same goal are different.

Table 5.23 - Breakdown of responses to the third question



India conceptualizes digital sovereignty primarily as a matter of state security, emphasizing national control over digital infrastructure and technological self-reliance.

Unlike market-driven or regulatory approaches, India's digital sovereignty discourse is predominantly shaped by geopolitical concerns and strategic dependencies on foreign tech giants and supply chains. Moreover, the Indian government is focused on leveraging the expansion of digital technologies as the key motor for economic growth. That would serve as the base for attracting foreign investments (Modi, 2024c) but only in a way that would allow Indian economic growth while respecting national security concerns.

Operationally, India balances regulatory interventions with protectionist industrial policies to enforce digital sovereignty. Regulation is mostly used to restrict the Big Tech dominance and hold foreign actors accountable while operating on Indian territory and managing data of Indian citizens. Protectionist measures, on the other hand, are evident in initiatives like the India Semiconductor Mission (ISM), the Production Linked Incentive (PLI) schemes, and MeghRaj Cloud (GI Cloud Initiative), all of which aim to build domestic technological capacity and protect national industries (Ministry of Electronics and Information Technology, Government of India, 2024). To conclude, The defining attributes of India's digital sovereignty claims are:

- security-driven policy making in digital sphere where digital sovereignty is framed as a strategic tool for national security and resilience
- interventionist industrial policies, focusing on self-reliance in AI and semiconductor where domestic production is protected from foreign competition
- strong control by the state over data and digital infrastructure

This approach positions India as an emerging tech power that prioritizes security and state control rather than open-market principles that are based on regulation and standards.

6. TTC and the Convergence and Divergence of Digital Sovereignty Discourses

6.1. The EU-India Comparison

Based on the previous analysis, both the EU and India are pursuing digital sovereignty in their actions, yet, their approaches differ significantly. Differences between the two exist due to different political positions and motivations on the global stage. In the first place, the EU is concerned with the critical dependencies that the Union is bound in digital spaces aiming to achieve technological independence, strategic autonomy, and value-driven innovation (Bria et al., 2025, p. 6). In the current political situation, the EU is also concerned with the impact of Big Tech, namely from the US and the efforts of the new Trump administration to affect the EU's legislation such as DSA (Windwehr, 2025).

On the other hand, India is concerned more with the security reasons rather than economic competitiveness. As the economy has a large population, Indian policymakers are trying to use the emergence of the digital economy as an opportunity for self-reliance. Moreover, where the EU is pushing for a rule-based framework through regulation such as the AI Act, DMA, or DSA, India is more bound to protectionist measures against multinational tech companies showing that both may see market concentration as the problem while differing in the means to tackle the issues. To compare the two digital sovereignty discourses, the key elements of both discourses will be analyzed.

Elements of the EU's Digital Sovereignty Discourse

The European Union conceptualizes digital sovereignty as a balance between economic competitiveness and security, framing it as a regulatory challenge rather than a national security imperative. The EU seeks to limit dependence on external technology providers while ensuring that its digital economy remains open, competitive, and aligned with European values.

Key elements are the following:

- A Balance between Economic Competitiveness and Security - The EU's digital sovereignty model does not prioritize state intervention in the digital economy. Instead, it relies on market regulations, competition laws, and supply chain diversification to create a fair and independent digital ecosystem. Moreover, the essential goal is to build European alternatives to reduce strategic dependencies while maintaining connection with global markets.
- Regulation as the Primary Mechanism - The EU leverages regulatory frameworks rather than direct state control to exert sovereignty over the digital space. As shown, standardization prevailed over protectionist measures especially regarding some of the critical documents such as the AI act and the European Strategy for Data.
- Strategic Autonomy over Critical Technologies - Namely in the semiconductor sector, documents such as The EU Strategic Dependencies and Capacities Report further emphasizes that Europe's digital sovereignty depends on diversifying suppliers, rather than isolating them from global trade.
- AI and other Emerging Technologies are regulated through a Trust-based framework - Foreign AI providers must comply with EU governance rules, reinforcing Europe's sovereignty without banning external AI models. The AI governance framework is further reinforced in the EC's AI policy, which promotes trustworthy AI while maintaining market competition.

Elements of the India's Digital Sovereignty Discourse

On the other hand, India's digital sovereignty discourse model is based on national security concerns, treating foreign tech dominance as a direct threat to state sovereignty. Unlike the EU's market-driven approach, India's framework is state-centric, emphasizing self-reliance, data localization, and strict foreign tech regulations. Key elements are the following:

- National Security is the Key Aim - Unlike the EU's balanced approach, India views digital sovereignty as a national security necessity rather than just a regulatory concern. Modi's speech at the Sydney dialogue and MeitY annual

report, among the analyzed documents, strongly advocate for the national security-oriented approach.

- State Control Over Data and Digital Markets - Unlike the EU, which relies on competition laws and regulatory governance, India enforces direct state intervention in digital markets. Documents such as the Digital Personal Data Protection Act and Digital India act lay down a strong framework for data localization and state oversight over digital platforms so that the government can control the development of crucial technologies.
- Self-Reliance over Global Integration - Unlike the EU's strategic autonomy model, India promotes absolute self-reliance in digital infrastructure. India Semiconductor Mission ensures domestic production of semiconductors, unlike the EU's supplier diversification strategy. Moreover, AI models that the Indian government is aiming to develop are indigenous-based differing from the European approach that allows foreign AI only if they respect European rules.

The EU and India are both actively pursuing digital sovereignty, but their approaches differ significantly due to distinct political motivations and strategic priorities. Both recognize the risks associated with foreign technology dominance and aim to reduce dependence on external tech providers. They also share concerns over market concentration, particularly by multinational Big Tech firms, and acknowledge the need to regulate digital markets and emerging technologies such as artificial intelligence and semiconductors. Additionally, both entities emphasize data protection, with the EU implementing regulatory frameworks like GDPR and the AI Act, while India enforces state-controlled governance through the Digital Personal Data Protection Act and the Digital India Act.

Despite these similarities, the EU and India diverge in their core motivations and regulatory mechanisms. The EU's digital sovereignty model seeks to balance economic competitiveness with security, ensuring that its digital economy remains open and competitive while reducing critical dependencies. In contrast, India's approach is primarily driven by national security concerns, with strong protectionist restrictions.

Accordingly, the role of the state in digital governance also varies between the two. The EU favors limited state intervention, focusing on legal frameworks and regulatory

oversight to shape its digital landscape. In contrast, India adopts a state-centric approach, with direct government control over digital markets and data governance. This distinction is also evident in AI and emerging technology regulation. The EU follows a trust-based framework, allowing foreign AI providers to operate as long as they comply with EU governance rules, reinforcing digital sovereignty without banning external AI models.

Areas of Convergence/Divergence

Based on the previous analysis, two essential areas have been identified in which the efforts of TTC could be helpful in converging digital sovereignty discourses:

- AI and Emerging Technologies - Both the EU and India share concern about the market concentration in the AI development field and their respective dependencies in the field, especially regarding the US and Chinese-based providers. Moreover, both of them promote responsible AI development, while their approaches, trust-based one in the EU (*EU AI Act*, 2023) and the self-reliant one in India (NITI Ayog, 2018a), are compatible for developing joint collaborations on AI safety and development.

- Semiconductor Supply Chain and Digital Infrastructure - Both the EU and India recognize their dependencies in the semiconductor field. India leans more toward self-reliance (Ministry of Mines, Government of India, 2023), the EU pushes for supplier diversification (European Commission, 2022) but both of them acknowledge the role of domestic production.

On the other hand, the analysis has shown that two of the following areas show very distinctive digital sovereignty discourse, thus limiting the potential of the TTC and converge them:

- Data Governance and Trade - India's state-centric, security-driven approach to data sovereignty conflicts with the EU's market-driven approach. Moreover, the EU sees data protection through the lens of consumers (*A European Strategy for Data*, 2020) while India pushes more towards national security (DPD Bill, 2023).

- Cybersecurity - India's approach to cybersecurity is state-centric (Ibidem) while the EU is more privacy-concerned (*The EU's Cybersecurity Strategy for the Digital Decade*, 2020).

6.2. Convergence

According to the constructivist theory, sovereignty, as well as its digital version embodied in digital sovereignty, is a socially constructed concept subject to constant changes as the opinions, values, and norms are being shared among participants (Adler, 2013). Following the constructivist logic, the EU-India TTC functions as a discursive space where digital sovereignty narratives are articulated, contested, and redefined. As the analysis has shown, two essential areas offer discursive convergence, while two others highlight fundamental divergences that limit the TTC's ability to align sovereignty claims.

AI and Emerging Technologies

In the first working group of the TTC, AI governance has been a recurring theme. Moreover, the group launched a multistakeholder AI initiative connecting key stakeholders from both sides (Delivorias, 2024). As both sides are framing digital sovereignty in AI as a response to US and Chinese market dominance, the setup of the AI initiative represents a functional arena where the slight differences could be lowered down and digital sovereignty understood as means of mitigating external dependencies.

Moreover, as both sides emphasize self-reliance in AI and emerging technologies development, the TTC has the potential to become an arena where the discourse is shifted towards strategic autonomy, focusing on joint AI safety regulations. These regulations could be adopted within or on the sidelines of the TTC meetings transforming the current defensive discourse to a more cooperative one between the two.

Semiconductors and Digital Infrastructure

Up to now, the TTC had a certain amount of success in restructuring the discourse on semiconductors as both sides signed the Memorandum of Understanding (Mou) during the second ministerial meeting in November 2023 (*India - EU TTC Working Group 2*

(WG2) on "Green & Clean Energy Technologies," 2024). Although both sides strongly push for reduction of their respective vulnerabilities in the supply chain, they frame sovereignty differently. The EU's discourse is more focused on supplier flexibility and open markets (European Commission, 2022) while India advocates for domestic production and national control over resources (Ministry of Mines, Government of India, 2023).

Within the TTC, the working group could serve as the bridge between two competing sovereignty framings under a shared goal of supply chain resilience. In other words, the TTC has the potential to be where discourse on semiconductors can be aligned justifying state support for semiconductor R&D without violating global trade norms.

6.3. Divergence

Regarding other two areas, the argument presented here is that TTC exposes sovereignty clashes in these areas, rather than resolving them. The source of the former lies in the fundamentally different ways in which the EU and India construct digital sovereignty in data governance and cybersecurity matters.

The EU's data governance approach is framed as a right-based issue as indicated by the European Strategy for Data and GDPR (*A European Strategy for Data*, 2020). More precisely, the EU regulations emphasize individual privacy, consent, and cross-border data flow if they're in line with regulations. India's approach on the contrary, is framed as national control over digital assets under the Data Protection Act (DPD Bill, 2023).

At the same time, both documents present opposite policy objectives for data governance. The EU's main objective is to ensure data protection of consumers and lower the power of Big Tech while making the single market more competitive. On the contrary, India pushes for strict data controls and the self-reliance approach (Ibidem).

The problems present in the data governance field are replicated to the cybersecurity issue. In the first place, their models are completely different as India pushes for state-driven control over networks and digital platforms (Kumar & Thussu, 2023). On the contrary, the EU's cybersecurity model is decentralized and focused primarily on consumer privacy and protection (*The EU's Cybersecurity Strategy for the Digital*

Decade, 2020). Ultimately, national security concerns present in India hinder cooperation as the country's position is strongly shaped by the geopolitical threats, namely from China. On the opposite, the EU focuses on cyber resilience and preventing corporate abuses rather than direct national security threats (Ibidem).

The stance on divergence is elaborated through the following arguments:

- The TTC is designed as a forum for structured discussion, but it lacks mechanisms for policy convergence where fundamental conflicts exist. Instead of harmonizing sovereignty claims, in these cases, the TTC becomes a space where the EU and India reaffirm their existing positions.
- Digital sovereignty is not a technical issue but it is also a political buzzword with different meanings (Pohle et al., 2024). As both sides use it to pursue different political objectives, the TTC becomes the arena where those goals are actively contested against each other.
- Broader geopolitical pressures undermine the TTC in these areas as actors beyond the EU and India are responsible for developments in the field, namely the US-China competition.

7. Concluding Remarks

This study has examined how the EU-India TTC functions as a discursive space where digital sovereignty narratives are negotiated, contested, and, in some cases, aligned. The analysis has provided a deeper understanding of how digital sovereignty is constructed and operationalized through political discourse, particularly from a constructivist perspective. By emphasizing the social construction of sovereignty through language and discourse, this research has explored the institutional, political, and geopolitical factors that shape digital sovereignty claims, revealing both areas of convergence and divergence in the digital sovereignty discourse between the EU and India.

As the word is getting more and more usage over the period of time, digital sovereignty is being widely explored through various different approaches and methodologies (Pohle et al., 2024). Before going into the intricacies of the EU-India relations, several concluding remarks around the discourse of digital sovereignty should be made. In the first place, the study reinforces the constructivist view that digital sovereignty is as much about political discourse as it is about technological capabilities, highlighting the power of language and institutional framing in shaping digital policy.

Secondly, the study has shown that digital sovereignty is not just a strategic policy goal related only to domestic policy but also a diplomatic tool that countries use to shape their relations to external actors. As shown in the case of the EU and India, digital sovereignty and closely connected discourse of strategic autonomy are widely used in the approach of both sides towards companies and other actors holding market power.

Thirdly and closely connected with the second point, digital sovereignty discourse is highly dependent on geopolitical situations, not only domestic policies. Digital sovereignty will be increasingly tied to global power dynamics. It will not just be a legal or economic issue but a geopolitical tool for shaping international digital governance and the attempt of emerging economies such as India, Brazil, and ASEAN countries to redefine their sovereignty through regional agreements.

One of the most important findings is that sovereignty does not always mean protectionism. On the other hand, just as in the case of AI and semiconductor fields in

the EU-India relations, sovereignty can be used to justify collaboration rather than isolation. This indicates that the potential digital sovereignty discourse depends on how actors choose to frame it (strategic autonomy or protectionism). As the study showed, the TTC was not capable of converging discourse only in the fields where the discourses were too distinct from each other.

Ultimately, future digital sovereignty strategies will likely be hybrid approaches, mixing state control, market regulation, and international partnerships rather than pursuing absolute digital independence. This study has shown the examples of such hybrid approaches as the EU combines regulation with global cooperation while India balances protectionism with selective partnerships through TTC, for example.

The findings of this study reveal that digital sovereignty has become a defining issue in the evolving EU-India relationship, shaping both their strategic alignment and policy divergences. While both actors seek to assert greater control over their digital ecosystems, their approaches to sovereignty are based on different priorities. The EU prioritizes regulatory autonomy and market governance, while India emphasizes state control and national security. The TTC has strengthened EU-India engagement by providing a structured platform for addressing key digital sovereignty challenges. In AI and semiconductors, sovereignty has been framed as a tool for trusted cooperation, leading to joint initiatives in AI safety and semiconductor resilience. These areas of convergence signal a broader strategic alignment between the EU and India as they seek to reduce dependencies on US and Chinese technology. However, other areas such as data governance and cybersecurity represent the bigger challenge as the two approaches are very distinct. Based on the discourse analysis of digital sovereignty and the TTC, three policy recommendations for the future work of the TTC have been singled out:

- ***To Expand AI and Semiconductor Cooperation Beyond R&D to Policy Coordination***
    - The EU and India should align AI regulatory principles to ensure interoperability between the EU AI Act and India's AI policies.
    - On semiconductors, the TTC should coordinate investment incentives and supply chain partnerships to reinforce a joint sovereignty framework against foreign suppliers.

- ***To Establish a Structured Mechanism for Data Governance Alignment***
    - Given the fundamental divergence in data sovereignty claims, the TTC should create a Data Governance Working Group that explores hybrid regulatory models.
- ***To Develop an EU-India Cybersecurity Coordination Framework***
    - Given the cybersecurity sovereignty divide, the TTC should introduce a cybersecurity risk-sharing mechanism focused on joint threat intelligence, cyber resilience, and critical infrastructure protection.

While similar studies in the field were dealing predominantly with the discursive analysis of digital sovereignty of only one actor, this study went beyond that by adding the second actor in the case, thus comparing them. Ultimately, the study added a significant element to discursive studies of digital sovereignty as it shed light on how a particular body, the TTC, can serve as a platform for exchanging and creating new discourses.

While this study has provided valuable insights into digital sovereignty discourse within the TTC, several limitations suggest areas for further research. This study relies on discourse analysis, but future research should integrate quantitative assessments like trade data, investment flows, and regulatory compliance metrics to measure the TTC's tangible impact on digital sovereignty policies. Moreover, future studies should examine how Big Tech, startups, and civil society influence TTC discussions, particularly in AI and cybersecurity to grasp the whole picture with all relevant stakeholders. Ultimately, a comparative analysis with US-EU, ASEAN, or China-led digital governance frameworks could reveal whether the TTC's approach is effective or adaptable globally.

References

28 June: EU-India summit – POLITICO. (n.d.). https://www.politico.eu/article/28-june-eu-india-summit/

30+ Top Tech Startups & Companies in 2024: Shaping the Future. (2024). StartUs Insights.

2030 Digital Compass: The European way for the Digital Decade. (2021). European Commission.

A European Strategy for Data. (2020). European Commission.

Adler, E. (2013). Constructivism in International Relations: Sources, Contributions and Debates. In W. Carlsnaes, T. Risse-Kappen, & B. A. Simmons (Eds.), *Handbook of international relations* (2nd ed, pp. 112–144). Sage.

Aghion, P., Cherif, R., & Hasanov, F. (2021). *Competition, Innovation, and Inclusive Growth*. International Monetary Fund (IMF).

Ankita, D. (2024). *India–EU TTC meet: Amping up the strategic partnership*. Observer Research Foundation (ORF). https://www.orfonline.org/expert-speak/india-eu-ttc-meet

Bahrke, J. (2022). *Commission internal digital transformation* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4199

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: Theory and cases. *International Relations*, *30*(4), 494–531. https://doi.org/10.1177/0047117815596590

Barlow, J. P. (1996). *Declaration of Independence of Cyberspace*.

Bava, U. S. (2021). India and the European Union: A Partnership for Joining Forces on

the Global Scene—Concluding Remarks and Outlook. In P. Gieg, T. Lowinger, M. Pietzko, A. Zürn, U. S. Bava, & G. Müller-Brandeck-Bocquet (Eds.), *EU-India Relations* (pp. 365–375). Springer International Publishing. https://doi.org/10.1007/978-3-030-65044-5

Bharti, S., & Singh, P. (2024, March 26). *EU Artificial Intelligence Act: Comparing India's approach with principles embedded in first of its kind EU legislation*. Bar and Bench - Indian Legal News. https://www.barandbench.com/law-firms/view-point/eu-artificial-intelligence-act-comparing-india-approach

Blackwill, R. D. (2024, June). *World Order is in a Downward Spiral*. CFR. https://www.cfr.org/article/world-order-downward-spiral

Breton, T. (2023a). *Digital Platforms as Regulated Entities: Our Single Market, our rules*. Annual Conference of the European Commission Legal Service, Brussels.

Breton, T. (2023b). *Industrial Strategy: We've come a long way (and it's only the beginning)*.

Bria, F., Timmers, P., & Gernone, F. (2025). *EuroStack – A European Alternative for Digital Sovereignty*. 127 p. https://doi.org/10.11586/2025006

Broeders, D., Adamson, L., & Creemers, R. (2019). *A coalition of the unwilling? Chinese & Russian perspectives on cyberspace*. Leiden University.

Budnitsky, S. (2022). A Relational Approach to Digital Sovereignty: E-Estonia Between Russia and the West. *International Journal of Communication*, *16*, 1918–1939.

Burgess, M. (2020). *Why the NHS Covid-19 contact tracing app failed | WIRED*. https://www.wired.com/story/nhs-tracing-app-scrapped-apple-google-uk/

Burwell, F., & Propp, K. (2022). *Digital sovereignty in practice: The EU's push to*

shape the new global economy. Atlantic Council.

Buzan, B., Wæver, O., & Wilde, J. de. (1998). *Security: A new framework for analysis*. Lynne Rienner Pub.

Carver, J. (2024). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy*, 1–37. https://doi.org/10.1080/13501763.2023.2295523

Chander, A., & Le, U. P. (2015). Data Nationalism. *Emory Law Journal*, *64*(3), 1–64.

Chaundhri, P. P. (2023). Delhi's new view of Europe: Opportunity for tech partnership? In V. Kranenburg & M. Okano-Heijmans (Eds.), *Clingendael Report*. https://www.clingendael.org/publication/strategic-tech-cooperation-between-eu-and-india#:~:text=Opportunities%20to%20enhance%20EU%E2%80%93India%20ties%20are%20analysed%20along,three%20areas%2C%20joint%20action%20with%20India%20is%20possible.

Chin, K. (2024). *What is the Digital India Act? India's Newest Digital Law | UpGuard*. https://www.upguard.com/blog/digital-india-act

Choi, C., & Yi, M. H. (2009). The effect of the Internet on economic growth: Evidence from cross-country panel data. *Economics Letters*, *105*(1), 39–41. https://doi.org/10.1016/j.econlet.2009.03.028

Choudhary, M. (2023, December 26). We want a Digital India. Just not the one we are living in. *The Indian Express*. https://indianexpress.com/article/opinion/columns/cyber-security-cyber-frauds-in-india-digital-india-data-protection-bill-9082569/

Christakis, T. (2020). *"European Digital Sovereignty": Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy*.

Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute.

Clayton, J. (2023). *TikTok CEO Shou Zi Chew's Congress showdown: Five takeaways*. https://www.bbc.com/news/65047087

Cogo Morales, P., & Jorge Ricart, R. (2023, February 24). *The EU-India Trade and Technology Council: Opportunities and challenges ahead*. Elcano Royal Institute. https://www.realinstitutoelcano.org/en/commentaries/the-eu-india-trade-and-technology-council-opportunities-and-challenges-ahead/

Commission approves 5 billion German State aid measure to support ESMC in setting up a new semiconductor manufacturing facility. (2024). EC - Press Release.

Couldry, N., & Mejias, U. A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, *20*(4), 336–349. https://doi.org/10.1177/1527476418796632

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

Dammann, F., & Glasze, G. (2023). Governing digital circulation: The quest for data control and sovereignty in Germany. *Territory, Politics, Governance*, *11*(6), 1100–1120. https://doi.org/10.1080/21622671.2022.2141850

Delivorias, A. (2024). *EU-India Trade and Technology Council* [At a Glance]. European Parliament Research Service.

Derek, G. (2024, May 29). *Europe's cybersecurity chief says disruptive attacks have doubled in 2024, sees Russia behind many*. AP News.

https://apnews.com/article/europe-election-cybersecurity-russia-ukraine-5b0cca725d17a028dd458df77a60440c

Digital Economy Report 2024. (2024). [Overview]. e United Nations Conference on Trade and Development.

Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control: The regulation of digital finance in the European Union. *Journal of European Public Policy*, *31*(8), 2226–2249. https://doi.org/10.1080/13501763.2023.2295520

Dunmire, P. L. (2012). Political Discourse Analysis: Exploring the Language of Politics and the Politics of Language. *Language and Linguistics Compass*, *6*(11), 735–751. https://doi.org/10.1002/lnc3.365

Ejdus, F. (2017). *Medjunarodna bezbednost: Teorije, Sektori i Nivoi* (Drugo izmenjeno i dopunjeno Izdanje). Fakultet Politickih Nauka - Univerzitet u Beogradu.

EU AI Act: First regulation on artificial intelligence. (2023, August 6). Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

EU-India Joint Press Statement. (2022, April). https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2643

EU-India: New Trade and Technology Council. (2023). [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_596

EU-India Relations | Bilateral Dynamics in an Evolving Global Order. (2023). European Foundation for South Asian Studies (EFSAS).

European Commission (Ed.). (2022). *EU Strategic dependencies and capacities: Second stage of in-depth interviews*.

European Commission (Ed.). (2023). *2030 Digital Decade: Report on the state of the Digital Decade 2023*. European Commission. https://doi.org/10.2759/318547

European Commission digital strategy Next generation digital Commission. (2022). European Commission.

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2022). *Digital Sovereignty—Rhetoric and Reality*. 1–14.

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: Towards digital sovereignty. *Journal of European Public Policy*, 1–27. https://doi.org/10.1080/13501763.2024.2309179

Floridi, L. (2021). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3827089

Gammeltoft-Hansen, T., & Adler-Nissen, R. (2008). An Introduction to Sovereignty Games. In R. Adler-Nissen & T. Gammeltoft-Hansen (Eds.), *Sovereignty Games* (pp. 1–17). Palgrave Macmillan US. https://doi.org/10.1057/9780230616936

Glen, C. M. (2014). Internet Governance: Territorializing Cyberspace? *Politics & Policy*, *42*(5), 635–657. https://doi.org/10.1111/polp.12093

Gu, H. (2023). Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese Political Science*. https://doi.org/10.1007/s11366-023-09855-1

Haass, R. (2022, May 10). *Is Diplomacy Between Russia and the West Still Possible? | by Richard Haass*. Project Syndicate. https://www.project-syndicate.org/commentary/diplomacy-between-russia-and-

west-during-ukraine-war-by-richard-haass-2022-05

He, G. (2022). The Narrative Turn in the Study of International Relations. *Academic Journal of Humanities & Social Sciences*, *5*(6). https://doi.org/10.25236/AJHSS.2022.050615

Heiskanen, J., & Beaumont, P. (2024). Reflex to turn: The rise of turn-talk in International Relations. *European Journal of International Relations*, *30*(1), 3–26. https://doi.org/10.1177/13540661231205694

Herrmann, R. K. (2013). *Perceptions and Image Theory in International Relations*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199760107.013.0011

Hilpert, H. G., Rudloff, B., & Wagner, C. (2023). *Negotiations on a Free Trade Agreement between India and the EU: Ambitions, expectations, obstacles, and incentives*.

India and the European Union in 2030: Building a Closer Economic Relationship (p. 158). (2023). Observer Research Foundation and Jacques Delors Institute.

India—EU TTC Working Group 2 (WG2) on "Green & Clean Energy Technologies." (2024). Office of the Principal Scientific Adviser to the Government of India. https://www.psa.gov.in/india-eu-ttc

Jackson, R. (1999). Sovereignty in World Politics: A Glance at the Conceptual and Historical Landscape. *Political Studies*, *47*(3), 431–456. https://doi.org/10.1111/1467-9248.00211

James, A. (1999). The Practice of Sovereign Statehood in Contemporary International Society. *Political Studies*, *47*(3), 457–473. https://doi.org/10.1111/1467-9248.00212

Jansen, B., Kadenko, N., Broeders, D., Van Eeten, M., Borgolte, K., & Fiebig, T. (2023). Pushing boundaries: An empirical view on the digital sovereignty of six governments in the midst of geopolitical tensions. *Government Information Quarterly*, *40*(4), 101862. https://doi.org/10.1016/j.giq.2023.101862

Jayaram, D. (2021). India's Climate Diplomacy Towards the EU: From Copenhagen to Paris and Beyond. In P. Gieg, T. Lowinger, M. Pietzko, A. Zürn, U. S. Bava, & G. Müller-Brandeck-Bocquet (Eds.), *EU-India Relations: The Strategic Partnership in the Light of the European Union Global Strategy* (pp. 201–226). Springer International Publishing. https://doi.org/10.1007/978-3-030-65044-5

Jorgensen, K. (2021). Low-Carbon Development: An Idea Whose Time Has Come-Unlocking Climate Cooperation Between India and the EU. In P. Gieg, T. Lowinger, M. Pietzko, A. Zürn, U. S. Bava, & G. Müller-Brandeck-Bocquet (Eds.), *EU-India Relations: The Strategic Partnership in the Light of the European Union Global Strategy* (pp. 185–200). Springer International Publishing. https://doi.org/10.1007/978-3-030-65044-5

Kamath, B. R. (2022). India and the European Union: A relationship yet to achieve its true potential. *Observer Research Foundation*.

Katasthane, P. (2023). Enhancing India-EU engagement on "meta-critical" technologies: A case for collaboration on semiconductors. In V. Kranenburg & M. Okano-Heijmans (Eds.), *Clingendael Report—How strategic tech cooperation can reinvigorate relations between the EU and India* (pp. 44–50). https://www.clingendael.org/publication/strategic-tech-cooperation-between-eu-and-india#:~:text=Opportunities%20to%20enhance%20EU%E2%80%93India%20ties%20are%20analysed%20along,three%20areas%2C%20joint%20action%2

0with%20India%20is%20possible.

Kohler-Suzuki, N. (2021). Determinants and Impediments of the EU-India Bilateral Trade and Investment Agreement: The Proof of This Old Pudding Is in the Eating. In P. Gieg, T. Lowinger, M. Pietzko, A. Zürn, U. S. Bava, & G. Müller-Brandeck-Bocquet (Eds.), *EU-India Relations: The Strategic Partnership in the Light of the European Union Global Strategy* (pp. 151–184). Springer International Publishing. https://doi.org/10.1007/978-3-030-65044-5

Kranenburg, V., & Okano-Heijmans, M. (2023a). How strategic tech cooperation can reinvigorate relations between the EU and India. *Clingendael Report*. https://www.clingendael.org/publication/strategic-tech-cooperation-between-eu-and-india#:~:text=Opportunities%20to%20enhance%20EU%E2%80%93India%20ties%20are%20analysed%20along,three%20areas%2C%20joint%20action%20with%20India%20is%20possible.

Kranenburg, V., & Okano-Heijmans, M. (2023b). The evolving role of technology: From business to strategic interest? In V. Kranenburg & M. Okano-Heijmans (Eds.), *How strategic tech cooperation can reinvigorate relations between the EU and India* (pp. 5–22). Netherlands Institute of International Relations 'Clingendael.'

Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.

Kumar, A., & Thussu, D. (2023). Media, digital sovereignty and geopolitics: The case of the TikTok ban in India. *Media, Culture & Society*, *45*(8), 1583–1599. https://doi.org/10.1177/01634437231174351

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, *60*(4), 3–26. https://doi.org/10.1177/0306396818823172

Lippert, B., Von Ondarza, N., Perthes, V., & Stiftung Wissenschaft und Politik. (2019). European strategic autonomy: Actors, issues, conflicts of interests. *SWP Research Paper*. https://doi.org/10.18449/2019RP04

Madiega, T. (2024). *Artificial intelligence act*. European Parliament Research Service.

Maheshwari, S., & McCabe, D. (2024). Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part. In *The New York Times*.

Martin, C. (2022). Geopolitics and Digital Sovereignty. In H. Werthner, E. Prem, E. A. Lee, & C. Ghezzi (Eds.), *Perspectives on Digital Humanism* (pp. 227–231). Springer International Publishing. https://doi.org/10.1007/978-3-030-86144-5

Mathiason, J., Mueller, M., Klein, H., & Holitscher, M. (2004). *Internet Governance: The State of Play*. The Internet Governance Project.

Mehrotra, P. (2022). *Here's a list of all the Chinese apps banned in India*. https://www.xda-developers.com/all-chinese-apps-banned-india/

Ministry of Communications (Ed.). (2018). *The National Digital Communication Policy*.

Ministry of Electronics and Information Technology, Government of India. (2024). *MeitY Annual Report 2023-24*. Government of India.

Ministry of Electronics and IT. (2023). *Proposed Digital India Act*.

Ministry of Mines, Government of India. (2023). *Critical MInerals for India*.

Modi, N. (2021). *PM delivers keynote address at The Sydney Dialogue, speaks on India's technology evolution and revolution*. The Sydney Dialogue.

Modi, N. (2024a). *Speech of Prime Minister Narendra Modi at the 18th Asia-Pacific Conference of German Businesses (APK) 2024*. 18th Asia-Pacific Conference of German Businesses (APK) 2024.

Modi, N. (2024b). *Today, India is the world's fastest-growing large economy, attracting global partnerships: PM*. News9 Global Summit, Stuttgart, Germany.

Modi, N. (2024c). *Today India is working in every sector, in every area with unprecedented speed: PM at NDTV World Summit*. NDTV World Summit.

Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? *Journal of European Public Policy*, 1–26. https://doi.org/10.1080/13501763.2024.2318475

Müller-Brandeck-Bouquet, G., Gieg, P., Lowinger, T., Pietzko, M., & Zürn, A. (2021). India and the European Union: A Growing Responsibility to Cooperate in a Changing World. In P. Gieg, T. Lowinger, M. Pietzko, A. Zürn, U. S. Bava, & G. Müller-Brandeck-Bocquet (Eds.), *EU-India relations: The strategic partnership in the light of the European Union global strategy* (pp. 3–18). Springer.

Nachiappan, K. (2024). Digital and Technology. In A. Sánchez-Cacicedo (Ed.), *EU-India relations: Gaining strategic traction?* (pp. 27–33). European Union Institute for Security Studies (EUISS). https://doi.org/10.2815/110238

Nayar, B. R. (1998). Political Structure and India's Economic Reforms of the 1990s. *Pacific Affairs*, *71*(3), 335–358. https://doi.org/10.2307/2761414

Nicole, A. (2024). *GAFAM Stocks: Definition, Market Influence, and Practical Insights for Finance Professionals*. SuperMoney. https://www.supermoney.com/encyclopedia/gafam-stocks

NITI Ayog. (2018a). *National Strategy for Artificial Intelligence*.

NITI Ayog. (2018b). *Strategy for New India @ 75*.

OECD. (2024). *OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier*. OECD. https://doi.org/10.1787/a1689dc5-en

Oxley, Z. (2020). Framing and Political Decision Making: An Overview. In Z. Oxley, *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1250

Panda, J. P. (2024). Trade, Connectivity and Supply Chains. In A. Sánchez-Cacicedo (Ed.), *EU-India relations: Gaining strategic traction?* (pp. 20–26). European Union Institute for Security Studies (EUISS). https://doi.org/10.2815/110238

Payne, R. A. (2001). Persuasion, Frames and Norm Construction. *European Journal of International Relations*, *7*(1), 37–61. https://doi.org/10.1177/1354066101007001002

Perarnaud, C., & Rossi, J. (2024). The EU and Internet standards – Beyond the spin, a strategic turn? *Journal of European Public Policy*, *31*(8), 2175–2199. https://doi.org/10.1080/13501763.2023.2251036

Pierri, P., & Herlo, B. (2021). Exploring digital sovereignty: Open questions for design in digital healthcare. *Design for Health*, *5*(1), 161–175. https://doi.org/10.1080/24735132.2021.1928381

Pinto, R. A. (2018). Digital sovereignty or digital colonialism? *SUR*, *27*.

Pohle, J. (2020). *Digital Sovereignty: A new key concept of digital policy in Germany and Europe* (pp. 3–26). Konrad Adenauer Stiftung.

Pohle, J., Nanni, R., & Santaniello, M. (2024). Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices. *Policy & Internet*, *16*(4), 666–671. https://doi.org/10.1002/poi3.437

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

Prasad Srichandan, S. (2021). *India-EU Broad-Based Trade And Investment Agreement*

(BTIA). Diplomatist. https://diplomatist.com/2021/05/15/india-eu-broad-based-trade-and-investment-agreement-btia/

Rakesh, V. (2022). Regulating Cross-Border Data Flow Between EU and India Using Digital Trade Agreement: An Explorative Analysis. In S. Schiffner, S. Ziegler, & A. Quesada Rodriguez (Eds.), *Privacy Symposium 2022* (pp. 105–128). Springer International Publishing. https://doi.org/10.1007/978-3-031-09901-4_7

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (2024).

Robinson, W. I. (1996). *Promoting polyarchy: Globalization, US intervention, and hegemony*. Cambridge University Press.

Saurugger, S. (2013). Constructivism and public policy approaches in the EU: From ideas to power games. *Journal of European Public Policy*, *20*(6), 888–906. https://doi.org/10.1080/13501763.2013.781826

Sinha, A. (2022). India in a changing global world: Understanding India's changing statecraft and Delhi's international relations. *The Round Table*, *111*(3), 398–411. https://doi.org/10.1080/00358533.2022.2087992

Soroos, M. S. (1986). *Beyond sovereignty: The challenge of global policy*. University of South Carolina Press.

Stiglitz, J. E. (2006). *Making globalization work: The next steps to global justice*. Allen Lane.

Tejasi Panjiar & Radhika Roy. (2023, August 5). Explained | What is the Data Protection Bill of 2023? *The Hindu*. https://www.thehindu.com/news/national/explained-what-is-the-data-protection-

bill-of-2023/article67162906.ece

Terzi, A., & Marcuzzi, S. (2019). Are multinationals eclipsing nation-states? In *IPS Journal*.

The Digital Personal Data Protection Bill, No. No. 113 (2023).

The EU-India Joint Action Plan. (2005, September).

The EU's Cybersecurity Strategy for the Digital Decade. (2020). EP and the European Council.

Thomas J., B. (2013). State, Sovereignty, and Territory. In W. Carlsnaes, T. Risse-Kappen, & B. A. Simmons (Eds.), *Handbook of international relations* (2nd ed, pp. 245–272). Sage.

Tripathi, S. (2021). India and the EUs Approach to Development Cooperation: Talking the Talk or Walking the Walk? In P. Gieg, T. Lowinger, M. Pietzko, A. Zürn, U. S. Bava, & G. Müller-Brandeck-Bocquet (Eds.), *EU-India Relations: The Strategic Partnership in the Light of the European Union Global Strategy* (pp. 227–252). Springer International Publishing. https://doi.org/10.1007/978-3-030-65044-5

Van Kersbergen, K., & Verbeek, B. (2007). The Politics of International Norms: Subsidiarity and the Imperfect Competence Regime of the European Union. *European Journal of International Relations*, *13*(2), 217–238. https://doi.org/10.1177/1354066107076955

Von der Leyen, U. (2019). *European Address.*

Von der Leyen, U. (2024). *Statement at the European Parliament Plenary*.

Wanger, C. (2008). The EU and India: A deepening partnership. In U. S. Bava, F. Zhongping, S. Fischer, M. A. Garcia, F. Godement, G. Grevi, D. Trenin, A.

Valladão, Á. de Vasconcelos, C. Wagner, G. Grevi, & Á. de Vasconcelos (Eds.), *Partnerships for effective multilateralism: EU relations with Brazil, China, India and Russia* (pp. 87–103). European Union Institute for Security Studies (EUISS).

Wendt, A. (1992). Anarchy is what states make of it: The social construction of power politics. *International Organization*, *46*(2), 391–425. https://doi.org/10.1017/S0020818300027764

Werner, W. G., & De Wilde, J. H. (2001). The Endurance of Sovereignty. *European Journal of International Relations*, *7*(3), 283–313. https://doi.org/10.1177/1354066101007003001

Williams, A. J., Hadfield, A., Rofe, J. S., & Rofe, S. (2012). *International history and international relations* (1. publ). Routledge.

Windwehr, S. (2025). *Trump vs. Europe: The role of the Digital Services Act | Heinrich Böll Stiftung | Brussels office - European Union*. https://eu.boell.org/en/2025/02/18/trump-vs-europe-role-digital-services-act