Michaela Vebrova

The European Digital Sovereignty Debate in the Context of Government Cloud Computing: Policies and Coalitions

Master Thesis

Submitted to the Chair for Information Systems and Information Management
(Westfälische Wilhelms-Universität, Münster)

for the Degree of Master of Science
in Public Sector Innovation and eGovernance (PIONEER)

Co-Supervisor 1: Prof. Dr. Joep Crompvoets
Co-Supervisor 2: Prof. Dr. Paul Timmers

Presented by: Michaela Vebrova
Lohweg 16
92369 Sengenthal
+49 152 0477 9772
michaela.vebrova@icloud.com

Date of Submission: 2022-12-09

Acknowledgements

Writing this thesis was an enjoyable and rewarding experience. For that, I would like to thank my supervisors, Prof. Dr. Joep Crompvoets and Prof. Dr. Paul Timmers, whose expertise and guidance have been extremely valuable, especially in the early stages of the process. Thank you very much for your time and energy, it has meant a lot to me.

I am also grateful to my former colleagues at the Joint Research Centre for encouraging me during my initial explorations of the subject and for not hesitating to connect me with interviewees to whom I would otherwise not have had access. I especially appreciate the generous help and mentorship of Dr. Sven Schade, Dr. Alex Kotsev, Dr. Robin Smith, and Dr. Jiri Hradec.

Special words of thanks also belong to my interview participants, who trusted me enough to share their thoughts on some of the EU's most controversial issues. As a byproduct, they also managed expose me to the highest professional standards embodied by European civil servants – that makes quite an impression on a graduate student!

I would also like to give a shout-out to two of my brilliant peers: my friend Thomas Balbach for his methodological advice and for being a classmate to look up to throughout the PIONEER program, and my co-adventurer María González Torres for convincing me that I cannot live without Mendeley and for being a source of inspiration as a young scholar whose work is always guided by her values and integrity.

Many people have supported me during the past four months on a personal level, but I am particularly thankful to W. H. and to the Focusmate community – especially Dr. K. & Dr. L. – for helping me use this thesis-writing exercise as an opportunity to develop a previously unknown degree of self-discipline. That is one of the greatest takeaways from this semester.

Table of Contents

List of Figures

List of Tables

List of Appendices

List of Abbreviations

ACF	Advocacy Coalition Framework
AI	Artificial Intelligence
AIOps	AI for IT Operations
APA	American Psychological Association
API	Application programming interface
APT	Advanced persistent threat
AWS	Amazon Web Services
BDN	The Blue Dot Network
BMW	Bayerische Motoren Werke
BPMN	Business Process Model and Notation
BRI	Belt and Road Initiative
BRICS	Brazil, Russia, India, China, and South Africa
CCP	Chinese Communist Party
CEO	Chief executive officer
CIA	Central Intelligence Agency
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CNE	Computer network exploitation
CPU	Central processing unit
CSP	Cloud service provider
CTO	Chief technology officer
C5	Cloud computing compliance controls catalogue
D9+	Digital Nine Plus
DGA	Digital Governance Act
DGRL	Digital Government Reference Library
DG CNECT	Directorate-General for Communications Networks, Content and Technology
DG DIGIT	Directorate-General for Informatics
DMA	Digital Markets Act
DNS	Domain Name System
DSA	Digital Services Act
DSR	Digital Silk Road
EC	European Commission
ENISA	European Network and Information Security Agency
ESCloud	European Secure Cloud
EU	European Union
EUCS	EU Cybersecurity Certification Scheme for Cloud Services
FaaS	Function as a service
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
GAFAM	Google, Apple; Facebook (Meta), Amazon, and Microsoft
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GLONASS	Global Navigation Satellite System
G7	Group of Seven
HR	Human resources
IaaS	Infrastructure as a service
IBM	International Business Machines
ICANN	International Corporation for Assigned Names and Numbers
ICT	Information and communications technology
IEC	International Electrotechnical Commission
IoT	Internet of Things

IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information technology
ITU	International Telecommunication Union
KPI	Key performance indicator
MS	Member State
MSCCG	Member States' Cloud Cooperation Group
NGO	Non-governmental organization
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OECD	Organization for Economic Co-operation and Development
OVH	Online virtual hosting
PaaS	Platform as a service
RO	Research objective
SaaS	Software as a service
SCC	Standard contractual clause
SCS	Special Collection Services
SLA	Service level agreement
SME	Small and medium-sized enterprise
SQL	Structured Query Language
SS	Search string
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TTC	Trade and Technology Council
UN	United Nations
URL	Uniform Resource Locator
U.S.	United States
WoS	Web of Science
ZTE	Zhongxing Telecommunications Equipment
5G	5th generation mobile network

1 Introduction

European governments undergoing digital transformation are facing two contradictory pressures, which are very difficult to reconcile. On the one hand, governments are striving to realize the benefits and possibilities offered by the latest technology, which includes cloud computing. Cloud computing allows the delivery of computing power and related capabilities via the Internet, thus saving governments significant costs while also improving service quality (Abied et al., 2022; McGillivray, 2022; Nanos et al., 2019). On the other hand, governments have the obligation to ensure that their citizens' data remain protected from unauthorized access. Nevertheless, an adequate level of security can be difficult to achieve when citizen data leave governments' data centers and migrate to the cloud, which may be physically located in a jurisdiction with weaker data protection laws, or it may be operated by a foreign entity that is subject to laws with extraterritorial application (Irion, 2012). Thus, in the cloud, virtual assets might be exposed to risks ranging from cyberattacks to cyber espionage (Couture & Toupin, 2019; Thumfart, 2020).

Member States of the European Union (EU) have been developing a range of policies and regulations to minimize such risks. A key narrative accompanying such policies has revolved around the concept of European digital sovereignty – the idea that states or governments in the EU should be able to reaffirm their authority over the digital realm (Musiani, 2022), in this case by taking measures to better control citizen data under their responsibility and the digital infrastructures on which the data is stored and processed. However, this control can be exercised in many ways, ranging from enforceable data protection and digital governance regulation to cloud cybersecurity certification schemes and well-negotiated contractual agreements. The problem is that not all public sector organizations in the EU share the same views regarding the preferred course of action (Kabelka, 2022). The most disagreement among Member States is provoked by proposed digital sovereignty policies that would view cloud service providers from third countries as inherently untrustworthy and practically disqualify them from certain types of contracts with public sector organizations in the EU (Kushwaha et al., 2020).

This thesis explores the causes of this assumed cleavage among Member States, the specific policies or initiatives where this disagreement occurs, and the advocacy coalitions formed by the participants of this debate. Focusing on a policy venue which has not yet been covered in the academic literature, this thesis offers behind-the-scenes insight into EU Member States' coordination efforts, whose end goal is to agree on a harmonized EU approach on public sector cloud computing. It is important to pay attention to it because when a common approach materializes, it will shape the ways in which all government organizations in the EU classify and store their citizen data in the years to come.

1.1 Research Aims and Objectives

The research question this thesis seeks to answer is: *What is the structure of the advocacy coalitions shaping the European digital sovereignty debate in the context of government cloud computing?* As explained in chapter 3, outlining an "advocacy coalition structure" entails more than just listing each coalition's members – the beliefs driving their policy preferences are also analyzed, thus providing an explanatory, and not just descriptive, research element.

To answer this question, the following sub-questions are asked, each corresponding with two or more research objectives (see Table 1.1):

- *In which ways are considerations about European digital sovereignty reflected in government cloud policies in Europe?* (Research objectives (ROs) 1-2)
- *What are the main points of debate among the stakeholders involved in formulating and implementing these policies?* (ROs 3-6)
- *Is there divergence among the stakeholders participating in this debate, and if so, what are some of the main factors producing this divergence?* (ROs 5-6)

RO No.	Research objective (RO)	Relevant chapter(s)
RO 1	Define the term "digital sovereignty" and understand its meaning in the EU context	*Chapter 2*
RO 2	Understand how the term maps onto the ongoing process of public sector cloud adoption	*Chapters 2 and 5*
RO 3	Identify the main stakeholders involved in formulating and implementing government cloud policies at the EU level and at the national level in two Member States	*Chapters 2 and 5*
RO 4	Identify the main policy venue(s) in which these stakeholders debate such policies at the EU level	*Chapters 2 and 5*
RO 5	Conduct at least 9 interviews with the stakeholders involved in these policy debates or in the implementation of these policies (3 at the EU level and 2x3 at the Member State level) to understand the main points of agreement and disagreement in relation to digital sovereignty, and the causes thereof	*Chapters 4 and 5*
RO 6	Outline the structure of the policy subsystem through the lens of the Advocacy Coalition Framework	*Chapters 3, 4, and 5*

Table 1.1 The research objectives of this thesis

1.2 Structure of the Thesis

The remainder of the thesis consists of five chapters. Chapter 2 is the literature review, where the term digital sovereignty is defined and public sector cloud computing is introduced, to then explore in depth the main policy problem at the heart of the European digital sovereignty debate regarding government cloud computing – the extraterritorial reach of certain pieces of U.S. legislation. Before discussing the gap in the literature, Chapter 2 briefly outlines the coordination efforts undertaken at the EU level and introduces a preliminary division of EU Member States into ones with a proactive and ones with a reactive approach to digital sovereignty.

Chapter 3 introduces the conceptual lens that is used in this thesis, namely the Advocacy Coalition Framework (ACF), and delves into the literature applying the ACF in order to devise a way of applying it that is suitable for the context of this thesis – a context of the intersection of national-level and EU-level policymaking.

Chapter 4 describes the methodology selected for this thesis. As the literature review is a major part of this work, the methodological part delves into the literature review strategy before moving onto the research design, research methods, and ethical considerations. The main data collection method of this thesis is a series of 13 interviews with policy actors participating in the policy debate.

Chapter 5 combines a presentation of the results of the interviews with a discussion. The findings are structured according to the main features of the Advocacy Coalition Framework, and three coalitions are identified: a proactive coalition (which draws a thick line between EU and non-EU cloud service providers in its digital sovereignty advocacy), a reactive one (which prefers the concept of "open strategic autonomy" over digital sovereignty to signal the need for the EU to remain open to its transatlantic partners), and a relatively neutral one (which might interpret the problem in a similar way as the first coalition, but prefers different solutions).

Chapter 6 concludes the thesis by discussing the significance of the findings and avenues for future research.

2 Literature Review

This chapter is divided into four sections. The first section outlines digital sovereignty in general and delves deeper into the European brand of digital sovereignty. The second section introduces cloud computing and discusses the role this technology plays in public sector digital transformation. The third section then ties the first two sections together by investigating European digital sovereignty in the context of government cloud computing. The last section highlights the gap in the literature this thesis intends to fill.

2.1 Digital Sovereignty

This section starts with a definition of digital sovereignty. The term is quite versatile; therefore, the process of deriving the working definition used in this thesis is shown. The term is further contextualized by outlining three main threats challenging governments' digital sovereignty. Next, the preferred definitions of other, closely related terms such as data sovereignty and strategic autonomy are presented. Thereafter, the European model of digital sovereignty is described by way of comparison with two other major models, the illiberal and the liberal one, with special attention to key government policies and legislation.

2.1.1 Definition of Digital Sovereignty

In this study, digital sovereignty is understood as "the ability of governments to control citizen data under their responsibility and the digital infrastructure on which the data is stored and processed." This subsection discusses the relevant literature to demonstrate how this definition was formulated, starting with broader definitions of digital sovereignty (which are more technically accurate or politically useful) before moving on to narrower ones (which are more practical for outlining the scope of a thesis).

Broader definitions. Digital sovereignty is often used as an umbrella term encompassing a variety of contexts impacted by digital technology, over which multiple (types of) stakeholders are competing to claim control. A typical example of a broad definition of digital sovereignty is "the sum of all abilities and possibilities of individuals and institutions to be able to exercise their role(s) in the digital world in an independent, self-determined and secure manner" (translation of Goldacker, 2017, in Lambach & Oppermann, 2022, p. 7). Adonis posits the term in a similarly expansive way, as "the idea of to what extent actors can control, govern, exercise, transfer, and use digital information, communication, and infrastructure" (2019, p. 268). Unpacking the word "digital," Floridi lists the most relevant contexts in which different actors battle for sovereignty: data, software, standards and protocols, processes, hardware, services, and infrastructures (2020, pp. 370–371). Building on Floridi's understanding, Roberts et al. define digital sovereignty as "a form of legitimate, controlling authority over – in the digital context – data, software, standards, services, and

other digital infrastructure, amongst other things" (2021, p. 6). The fact that such a vague definition is meant to encourage policymakers to use the term "in a more precise manner" (Roberts et al., 2021, p. 19), testifies to the term's severe fuzziness, whose acknowledgment is an obligatory starting point of any discussion of digital sovereignty.

Lambach and Oppermann's conclusion that "the concept is too multifarious and too "empty" to pin down within a single definition" (2022, p. 13) is a case in point. Yet, in the sphere of politics, upholding this "emptiness" is a strategic choice (Ruohonen, 2021). As Lambach and Oppermann (2022) go on to argue, it is precisely the interpretive flexibility of digital sovereignty that allows the concept to be invoked so frequently by such a plurality of political entrepreneurs, with many of the diverse narratives reinforcing each other in the minds of the public[1]. This is why definitions that aim to capture the political, normative connotation of the term (here marked in italics) also tend to be rather vague. For example, Thumfart characterizes digital sovereignty as "*the norm of* [emphasis added] national control over (…) digital technologies and their impact (…)" (2021, p. 3). Similarly, Musiani (2022) sees digital sovereignty as "the idea that states *should* [emphasis added] 'reaffirm' their authority over the Internet" and exercise their "self-determination in today's digital sphere" (p. 2). Such narratives may serve to legitimize different kinds of policies in different national contexts, from data protection regulations, through investment in innovation, to limits on Internet freedom (Christakis, 2020).

The term's usage in the academic literature is most systematically investigated by Hummel et al. (2021), whose rigorous review of a sample of 175 English and German publications maps the most common *agents*, *contexts*, and *values* associated with digital sovereignty. Being so comprehensive, their review is worth discussing in detail (with the caveat that only material published until November 2019 is covered). The *agents* that co-occur with digital sovereignty most frequently are countries (found in 109 publications), followed by governmental organizations (23 publications), private-sector organizations (17) and users/consumers (10); however, the list also includes agents as diverse as NGOs, inter-governmental organizations, and experts. The most common *contexts* digital sovereignty refers to in the reviewed sample are IT architecture (61), defense (42), and legislation (38), followed by societal discourse and advocacy, business and economy, and surveillance. Finally, the *values* associated with the term are control and power (85), security and non-maleficence (32), and deliberation, representation, and inclusion (19). The results of this review quantitatively demonstrate the fragmentation of the digital sovereignty debate. Still, although Hummel et al. (2021) refrain from doing so themselves, one could string together the "greatest common factors" among the agents, contexts, and values to approximate the most common notion of digital sovereignty. This approximation would read "a country's control and power over its IT architecture."

[1] At least in the context of German political discourse, where the term is particularly well-established

Narrower definitions. Narrow definitions of the term digital sovereignty tend to focus on state actors and their sphere of control or authority over digital technology (Adonis, 2019). Becerra and Waisbord explicitly refer to states enacting their "national interest" (2021, p. 69). State-centric definitions also equate sovereignty with autonomy (Prasad, 2022; Ruohonen, 2021), (regulatory or standard-setting) power (Becerra & Waisbord, 2021; Christakis, 2020; Glasze et al., 2022), intervention (Pohle & Thiel, 2020), or even domination (Prasad, 2022), but he word "control" is most common, probably thanks to its relatively neutral charge[2]. In line with this literature, the definition used in this thesis focuses on states – represented, more specifically, by their governments (seen both in the abstract, political sense, and as organizations) – as the main entity seeking to exercise control.

Some state-centric definitions emphasize the state's role as an agent of its citizens. For example, Thumfart's definition includes the elegant qualifier that "in nations that are legitimized by popular sovereignty", national control over digital technologies "indirectly includes the individual[3] control over digital technologies" (2021, p. 3). Similarly, one of Pohle and Thiel's definitions of digital sovereignty (2020) tasks governments with protecting "citizens and businesses from the manifold challenges to self-determination in the digital sphere" such as privacy issues, disinformation, or cybercrime (p. 2), or, as Shapiro puts it, the "societal effects" of digital technologies (2020, p. 7). The definition used in this thesis embraces this view by spotlighting governments' responsibility to protect the data of their citizens.

The last thing to clearly specify is the desired object of governments' control. While not exactly embracing this definition themselves, Moerel and Timmers note that digital sovereignty is often interpreted as the "ability of nation states to control the digital infrastructure on their territory and the data of their citizens," especially in the fields of cloud computing and social media (2021, p. 5). Likewise, Couture and Toupin, building on a 2012 reflection by Pierre Bellanger (an early champion of the term – *la souveraineté numérique* – in France), associate digital sovereignty with governments' and states' control over technologies and digital telecommunication networks, especially clouds for storing state and citizen data (2019). These definitions are very close to the direction taken in this thesis, as they also refer to citizen data and, notably, single out cloud computing as a key area with which digital sovereignty is concerned. However, what inspires the definition used in this thesis the most is their dual emphasis on infrastructure and data.

[2] For a definition of control endorsed in this thesis, see Floridi (2020, p. 371).

[3] Glasze et al. take this idea even further by portraying individuals as "digitally sovereign citizens" who contribute to their state's digital policy objectives (in the sense of enacting Foucauldian governmentality) by exercising their digital competencies (2022, pp. 19–21; cf. "individual empowerment narratives" in Lambach & Oppermann, 2022).

To recapitulate, the review of definitions of digital sovereignty found in the academic literature[4] has resulted in the formulation of the following working definition for this thesis:

> Digital sovereignty is the ability of governments to control citizen data under their responsibility and the digital infrastructure on which the data is stored and processed.

2.1.2 Threats to Digital Sovereignty from the Perspective of Governments

With the above definition centered around governments as a starting point, this subsection outlines three main dynamics shaping the "epochal struggle" for digital sovereignty (Floridi, 2020, p. 371), each entailing a different threat. The first dynamic is the private sector's dependency on technological solutions and services provided by the private sector; powerful private sector players may thus pose a threat to governments (Pohle & Thiel, 2020). The second dynamic is the increased utilization of digital surveillance tools by state actors in the context of the international system; there, governments may face the threat of cyber espionage coming from other governments and their agencies (Couture & Toupin, 2019; Thumfart, 2020). The third dynamic, which partially overlaps with the second one, relates to the fact that global connectivity enables malevolent actors to take advantage of cybersecurity vulnerabilities of organizations undergoing digital transformation; threats of cyberattacks targeting government organizations may originate from both state and non-state actors (Lambach & Oppermann, 2022; Mueller, 2020).

The actors involved. Before discussing each of these threats in more detail, it is useful to sketch out the relevant characteristics and relationships of the two central types of actors involved in this "struggle": states and large technology firms (Adonis, 2019). Governments' power lies mainly in their ability to regulate the digital realm and to (dis)incentivize different developments via taxation and public procurement policies, whereas Big Tech companies wield significant control over technological innovation and its applications, which they design, produce, sell, and maintain (Floridi, 2020). According to Pistor (2020), the power and governance structure of Big Tech companies[5] is in fact more akin to that of a small authoritarian state than that of traditional firms.

Two or more actors often form alliances based on common interests. For example, different EU states may partner up against a group of US companies that have acquired "de facto digital corporate sovereignty," as Floridi calls it, over the past two decades; alternatively, a governmental organization and a domestic company may join forces to challenge foreign political influence or economic competition (2020, pp. 371–372) or to create and implement

[4] In fact, the last two words of the working definition are not based on the literature review – the definition was amended at a later stage. As several experts interviewed for this thesis discussed the role of data in use and data in transit, it seemed apt to refer not only to storing, but also to processing data.

[5] This includes Internet platforms and online intermediaries (which are however not the focus of this thesis).

new technologies of surveillance (Lambach & Oppermann, 2022; Pistor, 2020). Against this background, the remainder of this subsection discusses the threats listed above, along with the main mitigation measures.

The threat of excessive dependency on specific private sector players. The digital sovereignty of state institutions and agencies undergoing digital transformation may be compromised by a disproportionate dependency on a small number of (domestic or foreign) IT technology and software providers (Lambach & Oppermann, 2022; Pohle & Thiel, 2020). The negative consequences of the worst case scenario – vendor lock-in (a very common problem in cloud services) – range from channeling public funds into overpriced services to being "stuck" with a software solution of a subpar quality or of suboptimal standards of data security or integrity (Opara-Martins et al., 2016). The causes of vendor lock-in include ill-advised contracts from the past and a lack of choice in the market (Lambach & Oppermann, 2022).

As a preventative or mitigation measure, governments may enact policies encouraging public administrations to use open-source software, stipulating public procurement rules and contractual agreements with encryption, data ownership, interoperability, or data portability requirements, or training civil servants to understand the above issues (Lambach & Oppermann, 2022; Moerel & Timmers, 2021). Alternatively, governments that have the capability to do so might decide to prohibit entrusting select services to private IT providers altogether (Carullo & Ernst, 2020), instead keeping the services under the wings of their own IT departments. In Carullo and Ernst's (2020) legal analysis, the principle of digital sovereignty is conceptualized as a national constitutional requirement that may be used to justify such prohibition. For example, they argue that outsourcing the storage of citizens' data to the private sector might be considered inadmissible in cases where it can be established that the state is unable to exercise its "enabling responsibility," i.e., if it cannot ensure that private IT service providers will safeguard public interest with respect to the availability, accuracy, appropriate use, and non-disclosure of data (Carullo & Ernst, 2020, p. 556). In extreme cases, citizens' fundamental rights and the state's own ability to perform its functions might be jeopardized. Generally, the state's level of enabling responsibility with respect to IT service providers is undermined by information asymmetries in favor of the companies, by weaker legal obligations imposed on private entities compared to public ones, and by the firms' profit motive and insolvency risk (Carullo & Ernst, 2020).

The threat of cyber espionage. Digital sovereignty is dramatically undermined when a foreign state or state-backed actor infiltrates a government IT system or a national telecommunications network and acquires data for peacetime espionage purposes (Floridi, 2020; Moerel & Timmers, 2021). The threat of cyber espionage may come from any country, whether hostile or allied[6] (Beim, 2018).

[6] In the European context, one of the most notorious examples is the United States' National Security Agency's (alleged) wiretapping of the German chancellor's email and phone communication.

To minimize the threat of cyber spying, governments may refrain from using international telecommunications networks wherever possible, instead raising their technological sovereignty (see also Table 2.1) by prioritizing the construction of domestic alternatives (e.g., localized data storage and email servers and cables, national clouds, or new undersea cables) (Maurer et al., 2015). In the case of concrete suspicions (combined with a lack of national capacity to build their own infrastructure), states may also put in place restrictions on the national origin of companies contracted by the government (Lambach & Oppermann, 2022). In addition, they may implement measures to improve their own resilience on the software front, e.g., by developing home-grown encryption solutions (Kaloudis, 2021). Lastly, digital sovereignty can be strengthened by reinforcing the power of domestic security agencies, improving the "legal and regulatory security architecture," and engaging in cyber foreign policy coordination (Lambach & Oppermann, 2022, p. 9).

The threat of cyberattacks. A related, but distinct type of a challenge to the digital sovereignty (and national security) of any state is the threat of attacks on government information systems, which may result in data breaches, the need to pay ransom, the disruption of government services, or even damage to physical infrastructure (Moerel & Timmers, 2021; Mueller, 2020; Ronquillo et al., 2018). These threats most often come from hostile state actors and financially motivated hacker groups.

To prevent such attacks, governments work to reduce the cybersecurity vulnerabilities of their IT systems and networks, such as by implementing robust user and network authentication and data encryption or by installing means of threat detection in all network devices; they also train their employees in good data and cyber hygiene, such as using strong passwords and recognizing email phishing (Pedreira et al., 2021; Ronquillo et al., 2018). Governments also ask their IT service providers to implement cyber defense and deterrence strategies (Thumfart, 2020). For example, as cloud servers, including those where government data is stored, are a particularly alluring target of APTs (advanced persistent threats) from both cyber criminals and state actors, the least governments can request from their providers is to implement cloud security monitoring solutions, allowing the timely detection and analysis of anomalous activity to prevent incidents (Moerel & Timmers, 2021).

2.1.3 Clarifying Related Terms

The literature dealing with sovereignty in the "realm of the digital" (Couture & Toupin, 2019) features a large array of partially overlapping or outright synonymous terms, depending on the author's preferred conceptualization[7] of the given notion (e.g., see Adonis, 2019, p. 267). Therefore, considering several of these terms in conjunction is common practice in the

[7] Many authors use these different terms interchangeably, thus perpetuating the blurring of conceptual boundaries between different notions of sovereignty (e.g., when Couture and Toupin arbitrarily rechristen the well-established term "indigenous data sovereignty" as "indigenous digital sovereignty" (2019)).

literature.[8] In the preliminary literature review stage, five terms interrelated with digital sovereignty were identified and four of them were later included as database search queries in the main literature review (see **Appendix J**). These terms are – in order of significance to this work – data sovereignty, technological sovereignty, strategic autonomy, cyber sovereignty, and network sovereignty. In a process analogous to that presented in subsection 2.1.1 (where a definition of digital sovereignty was "assembled" based on others), definitions of each of these related terms were delineated for this thesis, with the context of government cloud computing in mind. Table 2.1 below presents the results.

Term	Definition in this thesis *(+relation to digital sovereignty)*	Based mainly on
Digital sovereignty	"the ability of governments to control citizen data under their responsibility and the digital infrastructure on which the data is stored and processed"	Couture & Toupin (2019); Moerel & Timmers (2019)
Data sovereignty[9]	"governments' exclusive control over the access to all their virtual public assets, irrespective of where they are stored" *(a component of digital sovereignty)*	Irion (2012); McGillivray (2022); Zrenner et al. (2019)
Technological sovereignty	"the industrial capability and the presence of skills required to develop and produce critical technologies in a country" *(a precondition to digital sovereignty)*	Caravella et al. (2021); Kushwaha et al. (2020); Kaloudis (2021)
Strategic autonomy (or strategic sovereignty)	"the ability of states to independently make and execute decisions that affect their long-term national interest, especially with respect to their economy and society" *(a mutually reinforcing relationship with digital sovereignty)*	Timmers (2019); Christakis (2020); Ruohonen (2021); Roberts et al. (2021)
Cyber sovereignty	"the subjugation of cyberspace to national jurisdiction" *(digital sovereignty is a subset of cyber sovereignty)*	Maurer et al. (2015); Baezner (2018)
Network sovereignty	"the subjection of all physical networks and data within a state to government control and law enforcement" *(digital sovereignty is a subset of network sovereignty)*	Li & Yang (2021); Parasol (2018)

Table 2.1 Definitions of digital sovereignty and related terms used in this thesis

2.1.4 European Digital Sovereignty

The European model of digital sovereignty distinguishes itself in opposition to two other models – categories which were largely "invented" by the proponents of the European *third way*.[10] The European *regulatory* model has been characterized as a middle ground between the Chinese "heavy-handed state control model" and the "anarchic U.S. approach to digital

[8] For example, Hummel et al. start their review with "three cognate notions" of *digital*, *cyber*, and *virtual sovereignty*, only to later discover and include further notions including *internet* and *technological sovereignty* (2021, pp. 2–6). Similarly, Couture and Toupin focus simultaneously on *technological*, *digital*, *network*, *data*, *spectrum*, *computer*, and *information sovereignty* (2019, pp. 2306–2307). Others (e.g., Adonis, 2019; Musiani, 2022; Thumfart, 2021) take a similar approach.

[9] Another relevant definition focuses on control over cross-border data flows, in an effort to safeguard the confidentiality, integrity, and availability of sensitive data (Hummel et al., 2021; Nugraha et al., 2015).

[10] A loose fourth group can be created for Global South countries, where the digital sovereignty discourse is often framed as a struggle against digital (neo)colonialism – see for example Kwet (2019), Mann and Daly (2019), or Calzati (2022).

regulation" (Shapiro, 2020, p. 13); between "repressive authoritarianism" and "unchecked capitalism" (Lambach & Oppermann, 2022, p. 10); or between the "Chinese state-controlling authoritarian model" and the "American model of 'business above all'" (Charles Michel in Christakis, 2020, p. 86). In this thesis, this "bifurcation of Internet-based technologies along ideological divides" (De Gregorio & Radu, 2022, p. 69) corresponds with the distinction between the illiberal and the liberal models (Pigatto et al., 2021; Pohle, 2020), which are discussed in this subsection as a backdrop to the European *regulatory* model of digital sovereignty. Both domestic policy and foreign policy are considered. Given the global scope of this discussion, the broader definitions of digital sovereignty introduced in subsection 2.1.1 apply here.

2.1.4.1 The Chinese and Russian Illiberal Model of Digital Sovereignty

The illiberal model of digital sovereignty is closely related to network sovereignty, as defined in Table 2.1. Illiberal or authoritarian governments make no secret of interpreting their sovereign state power as a license to tightly control, restrict, and surveil the digital sphere, from infrastructure to online content (De Gregorio & Radu, 2022; Mueller, 2020). In doing so, they limit their ideological opponents' influence and business opportunities, while quelling domestic political dissent.

Domestic policy. Russia's pursuit of digital sovereignty resulted in the adoption of legislation mandating online platforms to provide intelligence services with decryption keys and backdoors to user data in 2016; in addition, 2019's Sovereign Internet Law – officially justified as a way to protect the country from cyberattacks – enabled the government to access and monitor data packages flowing across Russian borders (Daucé & Musiani, 2021; Glasze et al., 2022). The Sovereign Internet Law also initiated the creation of a national fork of the global Domain Name System (DNS), independent from and likely eventually uninteroperable with the existing system managed by the International Corporation for Assigned Names and Numbers (ICANN) – working towards what has been nicknamed as the "Splinternet" (Epifanova, 2020). This was a manifestation of Russia's long-standing view that the maintenance of Internet namespaces and numerical spaces should be shifted from the California-based NGO and multistakeholder group ICANN to an intergovernmental organization such as the UN's International Telecommunication Union (ITU) (Drezner, 2019; Mueller, 2020). Additionally, Roskomnadzor, Russia's national ICT and media regulator established in 2008, has used the guise of countering disinformation in Russia to heavily censor the online information space. Since 2014, the agency has been administering an Internet blacklist of URLs featuring forbidden "extremist content" (Maréchal, 2017), allowing it to silence government opposition. In 2020, the "anti-Apple law," as it became known, was passed, which required all smartphone devices sold in Russia to pre-install a compulsory set of Russian-made applications (Daucé & Musiani, 2021; van de Hoven et al., 2021). In the spring of 2022, international media started speaking of

a “digital iron curtain” when Roskomnadzor went on to block an unprecedentedly large number of domestic and international media outlets and popular social media including Facebook, Twitter, and Instagram (Chandran & Davydova, 2022).

Similarly, the “Great Firewall of China,” based on filtering mechanisms including IP and keyword-based blocking, denies users access to content deemed inappropriate by the Chinese Communist Party (CCP) (Lambach, 2020; Pigatto et al., 2021). The Cyber Security Law, which entered into force in 2017, requires information infrastructure and data collection operators to store Chinese citizens’ and residents’ data within the territory of mainland China and to grant the authorities full access to this data when a possible threat to national security is being investigated (Parasol, 2018).

Foreign policy. In the 2010s, the governments of Russia and China, in collaboration with their leading digital media companies (Yandex and Baidu, respectively), formed an alliance in opposition to what they explicitly referred to as the United States’ hegemony in Internet technology and governance (Budnitsky & Jia, 2018). Russia and China’s shared position, developed at various international summits and forums including the UN and formalized with a bilateral agreement in 2015, has been framed as a quest for Internet sovereignty. Corresponding to Table 2.1’s definition of cyber sovereignty, Internet sovereignty is the idea that cultural and political differences among countries should be respected and reflected in different national Internet governance regimes (where, as shown above, illiberal governments tend to favor a significantly more content-restrictive approach within their territories and prefer multilateralism over multistakeholderism in the international arena) (Budnitsky & Jia, 2018; Couture & Toupin, 2019; Wenhong, 2020). Sino-Russian efforts to challenge the ICANN-led Internet governance model, have also been supported by smaller illiberal players such as Iran and Cuba (Thumfart, 2021).

The Chinese government’s efforts to reshape the global digital order are not limited to political arenas. Realizing its ambition to become a global “cyber superpower” (Pohle & Voelsen, 2022), China is successfully projecting its power internationally through President Xi’s signature Belt and Road Initiative (BRI). The initiative’s Digital Silk Road (DSR) agenda, announced in 2015, entails infrastructure investments in fiber-optic cables and network equipment, satellite systems, smart cities, or quantum and cloud computing centers across six continents, “primarily in the ‘developing world’” (Woon, 2021, p. 287). While the BRI is likely to substantially contribute to closing the digital divide, Woon argues that DSR infrastructures are also likely to be used as surveillance systems furthering Chinese geopolitical interests (2021). Crucially, China is also using the DSR to challenge Western digital hegemony through standard-setting. As outlined in the “China Standards 2035” strategy, China is pushing for a new generation of information technology standards in areas ranging from 5G to “new cloud computing” and “new artificial intelligence,” and it is likely

that adherence to these standards will be a prerequisite to future infrastructure investments across the DSR network (de La Bruyère & Picarsic, 2020, pp. 19–22; Woon, 2021).

2.1.4.2 The American Liberal Model of – Internet Freedom?

The second model, at the most liberal end of the spectrum, is associated chiefly with the United States (U.S.), the originator of the multistakeholder model of Internet governance and an advocate of a laissez-faire approach to regulating the digital economy (Glasze et al., 2022; Lambach & Oppermann, 2022; Lantis & Bloomberg, 2018). Accordingly, the digital sovereignty discourse is mostly absent in the U.S., with the seemingly opposing narrative of "Internet freedom" being more prevalent (Burwell, 2020; Couture & Toupin, 2019). Couture and Toupin explain this by observing that calls for more sovereignty are stronger wherever there is a perception that authority is weak; hence, the country that remains "the Internet's power center" has fewer reasons to invoke the notion of digital sovereignty (2019, p. 2310).

Domestic policy. The Internet freedom narrative portrays the digital sphere as an immaterial, territorially unbound, and anarchic space, which should be guarded against undue government interference – thereby distracting from the reality of the "physical infrastructure located in specific geographies and jurisdictions" (Mainwaring, 2020, p. 215). The software and hardware architecture underpinning the American technosphere – from the algorithms powering the most popular social media platforms to the intercontinental network of submarine data cables – is largely in the hands of the Big Five or "GAFAM" companies (Google/Alphabet, Apple, Facebook/Meta, Amazon, and Microsoft), which have managed to fend off public oversight and consolidate considerable power to decide the "technical and behavioral rules" structuring the digital realm (De Gregorio & Radu, 2022, p. 75). Thus, the U.S. has seen a "hybridization" of its Internet governance, where the public sector has de facto delegated some of its regulatory functions to private actors that are free to "define and interpret users' fundamental rights according to their legal, economic, and ethical frameworks" (Chenou & Radu, 2019; De Gregorio & Radu, 2022, p. 78). As evidenced by the Cambridge Analytica scandal, such frameworks have prioritized the pervasive extraction, analysis, and commodification of data (Schneider, 2020), including data about citizens' (past and future) online behavior (Zuboff, 2015). Thus, U.S. technology companies have inadvertently invented what Zuboff calls "surveillance capitalism" – in her view, a largely anti-democratic form of control that has materialized behind the smokescreen of Internet freedom narratives (2015).

However, some authors believe that it would be a mistake equate the U.S. government's support for industry self-regulation with powerlessnes vis-à-vis the Big Tech corporations. Schneider argues that one of the reasons why the government has not been overly eager to constrain the Big Five's data collection practices is that it has sought to use the data for its own purposes (2020). 2013's revelations by the whistleblower Edward Snowden showed that the U.S. National Security Agency (NSA) was in fact one of the world's main infringers on digital

sovereignty, with direct access to bulk data from the servers of Apple, Facebook, Google, Microsoft, Yahoo, or YouTube – under the Foreign Intelligence Surveillance Amendments (FISA) Act of 2008, the companies were legally required to enable the agency to circumvent their encryption and privacy controls (Lyon, 2014). In addition, the Snowden disclosures described the NSA's fiber optic cable tapping apparatus called "Upstream," through which the agency could intercept any internet traffic (Lyon, 2014). According to Schneider, the purpose of NSA's surveillance was not limited to combating terrorism and other types of criminal activity[11] – the agency also used the data for economic espionage and "gains in international diplomacy" (2020, p. 10). While many states are known to have sophisticated foreign cyber espionage programs (cf. Lemay et al., 2018), Snowden's revelations about the extent of NSA's surveillance shocked the world, undermined global trust in an Internet shaped in the United States' image, and reinforced digital sovereignty narratives elsewhere, particularly in the EU (Lambach & Oppermann, 2022). Countries worldwide have consequently started paying increased attention to the geopolitics of the undersea cable system; for example, the BRICS countries (Brazil, Russia, India, China, and South Africa) have announced they would build their own submarine cable network in order to reduce their dependence on the West and decrease the risk of surveillance (Bueger & Liebetrau, 2021).

Foreign policy. The United States has taken a firm stance against China's challenge to its global technological primacy, thereby entering a "digital cold war" (Shen, 2016; Woon, 2021), also termed the "tech cold war" (Oertel, 2020). The U.S. effort to preserve its global role commonly uses the "freedom versus authoritarianism" trope. In April 2020, the U.S. Department of State announced the Clean Network program, whose stated aim was to address "the long-term threat to data privacy, security, human rights and principled collaboration posed to the free world from authoritarian malign actors" such as the CCP (US Department of State, 2021). As part of this initiative, the U.S. persuaded dozens of its "freedom-loving" allies (labeled "Clean Countries") to prohibit Huawei, ZTE, and other Chinese companies from supplying 5G infrastructures in their territory (Bueger & Liebetrau, 2021). The U.S. had done the same through its "Huawei ban" (which also concerned dozens of other Chinese companies deemed to pose national security risks). The ban was approved by the Congress during the Trump presidency (the Secure and Trusted Communications Networks Act of 2019) and extended during the Biden presidency (the Secure Equipment Act of 2021). In August 2020, the U.S. Department of Commerce also prohibited the unlicensed sale of semiconductor chips developed using U.S. technology to Huawei (Moerel & Timmers, 2021). In the same month, U.S. President Trump issued an executive order – subsequently blocked by a federal judge – that would ban the Chinese video-sharing mobile application TikTok, alleging that the CCP may use the application to collect U.S. citizens' personal information

[11] The leak also contained a map showing over 50,000 computer network exploitation (CNE) implants and over 80 sites of the Special Collection Services (SCS) program, which focuses on installing eavesdropping equipment targeting governments around the world (Mueller, 2020).

and blackmail them, conduct corporate espionage, or censor politically sensitive content, thus threatening the national security and economy of the U.S. (Federal Register, 2020).

A large component of U.S. cyber foreign policy is deepening Washington's ties with its Western allies. In April 2022, the U.S. and around 60 international partners including all EU Member States put forth a Declaration for the Future of the Internet, with a vision to "resist efforts to splinter the global Internet" by protecting the multistakeholder system of Internet governance, to increase the trustworthiness of network infrastructure and service suppliers, and to safeguard fundamental freedoms, including by refraining from using techniques for unlawful surveillance (2022, pp. 1–3). In June 2021, the EU-US Trade and Technology Council (TTC) was formed as a forum for cooperation on technology issues including technology standards, secure supply chains, and data governance. In September 2021, weeks before the inaugural meeting of the TTC, the U.S. rallied the transatlantic community around "trusted connectivity" – the idea that democratic countries should ensure that their values (from sustainability to human rights) be baked into their digital infrastructure, otherwise "autocratic governments" will set the rules as they see fit (Noyan, 2021). One of the key mechanisms for implementing this principle is the Blue Dot Network (BDN), initiated by the U.S., Japan, and Australia in November 2019 and later endorsed by various U.S. partners, the G7 (as part of its Build Back Better World initiative), and the OECD. The BDN will be a certification of excellence scheme aiming to promote investment in infrastructure projects that satisfy criteria of transparency, accountability, environmental sustainability, rule of law, and human rights protection (US Department of State, 2022). It is seen as the West's response to China's BRI.

2.1.4.3 The European Value-Based Model of Digital Sovereignty

European digital sovereignty is based on the EU's own *rules*, which stem from European *values* (Celeste, 2021; Glasze et al., 2022; Kaloudis, 2021; Lambach & Oppermann, 2022; Roberts et al., 2021; R. D. Taylor, 2020). The European approach is presented as an alternative to the two models outlined above and, by extension, as an alternative to the "products and services offered by non-European multinationals" currently dominating the EU's digital market, "consequently imposing their values and rules" (Celeste, 2021, p. 7). European *values* can be gleaned from related EU policy documents – political statements about European digital sovereignty rarely specify these. In the digital context, an especially relevant document is the European Commission's proposed European Declaration on Digital Rights and Principles for the Digital Decade, which seeks to promote a digital transition based on European values by focusing on human-centered technology; solidarity and inclusion; freedom of choice in the online environment (especially in interactions with AI); participation in the digital public space; safety; security and empowerment (which includes data privacy and protection from cybercrime and data breaches); and sustainability (so digital devices

support the green transition) (2022e). There is a long list of relevant *rules* enforcing these values in the name of European digital sovereignty. Tellingly, Christakis (2020) conceptualizes European digital sovereignty mainly as the EU's "power to regulate" the digital space and the tech sector (p. 11).

The idea of European digital sovereignty allows for the transposition of the typically state-centric notion of sovereignty to the level of the European Union[12]. Recalling the broader definition of digital sovereignty by Roberts et al., quoted in subsection 2.1.1, sovereignty can be understood as "a form of legitimate, controlling authority (…)" (2021, p. 6). This authority can be held not only by states, but also by "international or supranational bodies" such as the EU[13] (Roberts et al., 2021, p. 7). Yet, for absolute clarity, let it be stressed that the word "European" in European digital sovereignty refers to a particular model of digital sovereignty that is advanced by both national-level and EU-level policymakers; it is therefore not to be associated chiefly with the EU. After all, it was initially promoted by representatives of France and Germany.

Domestic policy. Given that EU policymakers often use the terms digital sovereignty, technological sovereignty, and strategic autonomy interchangeably[14] (Adonis, 2019; Calderaro & Blumfelde, 2022), it is not surprising that there is a plethora of EU policy initiatives that are presented as measures to make Europe and its Member States more digitally sovereign. Based on their analysis of the three main EU institutions' websites, Roberts et al. (2021) identify five policy areas where the EU refers to digital sovereignty: data governance, constraining platform power, digital infrastructure, emerging technologies, and cybersecurity. Barrinha and Christou (2022) recognize as many as eight groups of European digital sovereignty policy tools, from public procurement to research and development. The below overview focuses on the most important policy initiatives fostering European digital sovereignty. With the subject of this thesis in mind, it pays special attention to different measures' relevance to the cloud computing industry.

Related also to the values of human dignity, security, non-discrimination, and empowerment, the fundamental rights to consumer protection, privacy, and protection of personal data are well-established in European legal history (Burwell, 2020; Zygmuntowski et al., 2021). The

[12] Speaking of sovereignty in relation to anything other than Member States was considered inappropriate just five years ago, but the political climate has changed (Timmers (2020) in Christakis, 2020).

[13] The authors also usefully clarify that digital sovereignty understood as a form of legitimate, controlling authority can be shared "across political communities and spatial networks" (Roberts et al., 2021, p. 7) or "pooled" (Floridi, 2020, p. 377; Moerel & Timmers, 2021, p. 23). When Member States join forces in the fight against cross-border cyber threats (against which they are too weak individually), they strengthen their national sovereignty (Moerel & Timmers, 2021). Following this conceptualization, this thesis views European digital sovereignty as something that can be held by multiple agents at multiple levels at once, i.e., both by individual EU Member States and the EU as a whole.

[14] Csernatoni makes the insightful observation that "mainstreaming a security imaginary" into "various lower-level policy fields across tech and digital policy" is a rhetorical strategy aiming to enhance their strategic priority and open policy windows of opportunity (2022, p. 395).

EU asserted these values through one of the most significant pieces of legislation of the digital era when it adopted the General Data Protection Regulation (GDPR) in 2016 (which then took effect in 2018). The GDPR gave the EU the strongest data protection regime in the world by, for example, introducing the right to the erasure of personal data (also known as the right to be forgotten), the right to data portability, the prohibition of data collection (or data mining) without the data subject's informed consent, or new minimum standards regarding the security, processing, and sharing of personal data (Calderaro & Blumfelde, 2022; Gstrein & Zwitter, 2021; Gueham, 2017; Schneider, 2020). The Regulation also brought issues related to personal data sovereignty to the forefront of Europeans' consciousness.

The European strategy for data (2020) emphasizes security, data protection, energy efficiency, and fair and trustworthy market practices. A set of EU-wide measures facilitating cross-border data flows and encouraging data sharing (and reuse) seeks to balance protecting individual privacy rights with maximizing the economic and innovation potential of data (Celeste, 2021; Roberts et al., 2021; Zygmuntowski et al., 2021). These measures include 2018's Single Digital Gateway Regulation, 2018's Regulation on the Free Flow of Non-Personal Data, 2019's Open Data Directive establishing new rules on high-value datasets, 2022's Data Governance Act (DGA), and the public services-focused Interoperable Europe Act, proposed in November 2022. Especially the DGA, which will be applicable from September 2023, is seen as a "key text for digital sovereignty" (Christakis, 2020, p. 77). The most relevant part of the DGA is Article 31 – International access and transfer –, where service providers are obligated to take all reasonable measures to prevent international transfer or governmental access to non-personal data (effectively a data localization clause) (European Commission, 2022d). The Regulation also empowers individual citizens and companies to exercise their data sovereignty by making use of a new mechanism for data altruism (Hummel et al., 2019). Crucially, the DGA will also facilitate the creation of so-called Common European data spaces – ecosystems for sharing interoperable data in strategic domains (ranging from health to energy), involving both private and public sector data (Christakis, 2020). The DGA is going to be complemented by the proposed Data Act, which seeks to promote fairness in the access and usage of non-personal data by creating a harmonized framework on who can access and use what data, thus giving consumers more control over the data generated by their activities (including more effective ways of switching between different cloud data processing service providers) (2022c). (Another significant contribution to the creation of the next generation of trusted data infrastructure is the GAIA-X association, a network of cloud service providers, based on a common reference architecture and standards, facilitating secure and sovereign data exchanges between participating organizations (Braud et al., 2021) (see also section 2.3.2).

Other, recent pieces of legislation reflect the EU's human-centric approach to the digital economy (while improving market competitiveness). In November 2022, two major EU Regulations entered into force, which introduced new responsibilities for platforms with the

power to act as rule-makers or gatekeepers in online markets – the Digital Markets Act (DMA) and the Digital Services Act (DSA). The DMA, which will start applying in May 2023, covers ten core platform services ranging from online search engines to cloud computing services, and the obligations it imposes on gatekeepers include ensuring data portability and allowing third parties to interoperate with their services. (Roberts et al., 2021) The DSA gives the European Commission new supervisory powers, including via the newly created European Centre for Algorithmic Transparency, which will audit very large online platforms' and search engines' algorithmic systems to ensure their trustworthiness. The DSA also imposes four tiers of due diligence obligations on the providers of intermediary and hosting services, online platforms, and search engines (Husovec & Roche Laguna, 2022; Renda, 2021). For example, hosting services, which include cloud services, are obligated to notify the authorities if they become aware of manifestly illegal content (Husovec & Roche Laguna, 2022). Next, the proposed Artificial Intelligence Act (AI Act; expected to be passed in 2023) also takes a value-based and risk-based approach, subjecting high-risk applications of AI to strict obligations such as providing users of AI systems with adequate information to protect their dignity and freedom of choice, or ensuring human oversight and the use of high-quality data sets to minimize the risk of discrimination. These Acts, which are expected to empower European digital consumers and foster the growth of European SMEs while slowly reducing the dominance of U.S.-based tech giants, are seen as a significant step towards European digital and technological sovereignty (Burwell, 2020; European Economic and Social Committee, 2021; van de Hoven et al., 2021).

There are also several key industry-focused measures aiming to boost European digital sovereignty by enhancing its technological sovereignty and strategic autonomy[15] (Timmers, 2022a). The goal is to decrease Europe's dependency on third country suppliers of critical technologies, from 5G/6G equipment to semiconductors (Timmers, 2022a). The latter is addressed by European Chips Act, proposed in February 2022 (and expected to be passed in early 2023), which includes ambitious funding mechanisms and investment in fabrication plants that are hoped to help double the EU's global market share in semiconductors (from 10% to 20%) (Codagnone et al., 2021; Sheikh, 2022). European values are embedded in the Act via proposed certification for energy-efficient and trusted chips (European Commission, 2022a). Such initiatives will be greatly reliant on strategic partnerships between the private and public sectors, in this context also called strategic autonomy tech alliances, anchored in technological, industrial, and political drivers (Timmers, 2022a).

[15] Important strategic autonomy measures that cannot be discussed in detail in this subsection due to space constraints include the European High Performance Computing Joint Undertaking; the proposed Regulation establishing the Union Secure Connectivity Programme for the period 2023-2027, relying on satellite infrastructure and quantum encryption technologies; or the proposed Roadmap on critical technologies for security and defense (Codagnone et al., 2021). These measures parallel similar efforts elsewhere – for example, the Chinese "indigenous innovation" efforts (Zhao, 2010), which have produced the BeiDou Navigation Satellite System (as an alternative to the US GPS or the Russian GLONASS), state-of-the-art 5G technology and infrastructure, leading e-commerce and social media platforms, a number of patents related to blockchain technology, or a growing global market share in cloud computing and Internet of Things markets (Pigatto et al., 2021; Yan, 2020).

Lastly, strong cybersecurity is seen as a cross-cutting issue supporting the quest for digital sovereignty by protecting Europe's data, infrastructures, and businesses (Roberts et al., 2021). Key measures include 2016's Network and Information Security (NIS) Directive (which introduced new obligations for digital service providers – including cloud computing providers – to report cybersecurity incidents to government authorities) and 2019's Cybersecurity Act (which, among other things, gave an impulse for the creation of an EU cybersecurity certification scheme for cloud services – see subsection 2.3.2) (Christakis, 2020; Codagnone et al., 2021; Roberts et al., 2021). Lastly, the European Cyber Resilience Act, proposed in September 2022, focuses on the transparency of security properties of products with digital elements (European Commission, 2022b).

Foreign policy. Even if they are not framed as foreign policy initiatives, many EU regulations pursuing sovereignty in the digital realm inevitably have a worldwide ripple effect – also known as the "Brussels effect," a form of soft power whereby the EU's relatively strict regulatory regime sets global norms and standards (Christakis, 2020; Schneider, 2020; cf. Bradford, 2012). For example, some GDPR provisions are applicable anywhere in the world, as long as the personal data of a European citizen are involved (Barrinha & Christou, 2022). Facing the threat of fines of up to €20 million or up to 4% of their global annual turnover for the most serious violations, multinational tech companies operating in Europe have had to invest in capabilities ensuring compliance[16] – measures which they often extend to their worldwide operations (either voluntarily or because it is not practical to have multiple versions of their products in different regions) (Christakis, 2020). This export of EU values via EU regulations has been described as a "global game changer" (Schneider, 2020, p. 12), celebrated by those who subscribe to these values, as it is claimed to "serve global welfare" by replacing the "self-serving" approach advanced by the U.S. with a vision of a "rule-based world" (Bradford (2020) in Christakis, 2020, p. 15).

Nonetheless, others criticize the Brussels effect as a global projection of European hegemonic power through regulations with a de-facto extraterritorial effect (Gstrein & Zwitter, 2021), or in other words as "unilateral regulatory globalization" (Bradford (2020) in Christakis, 2020, p. 22). Celeste notes that Europe's American partners may understandably view *normative power Europe* in the field of data protection as a "form of imperialism," which erodes the digital sovereignty of Europe's global players (2021, p. 14). Farrand and Carrapico (2022) make a similar argument in relation to EU cybersecurity policy, asserting that the digital sovereignty discourse of the von der Leyen "geopolitical Commission" in fact pursues a regulatory mercantilist approach to cybersecurity governance, where (only) European businesses qualify as "champions of EU norms and values," just by virtue of their geographic location (p. 450). Likewise, Calderaro and Blumfelde (2022) focus on European AI policy (similarly to the

[16] Nonetheless, Renda (2021) and Bodó et al. (2021) point out Big Tech firms' ability to circumvent the GDPR and discuss the difficulty of ascertaining non-compliance.

GDPR, the proposed AI Act (European Commission, 2022f) also has extraterritorial application, as its scope includes cases where the provider or the user of a service is located in a third country). They believe that the externalization of the EU regulatory agenda is a "protectionist strategy" adopted as a result of the realization that European companies lag behind their global competitors in the AI domain and are unlikely to catch up in the near future (Calderaro & Blumfelde, 2022, p. 420). Lastly, according to Renda (2020), the creation of GAIA-X marks another phase in "Europe's regulatory expansionism" (p. 60). To be able to provide cloud services in the EU, operators will have to adhere to a set of protocols and standards that embed compliance with key EU policies ranging from the European data strategy to the GDPR, the Cybersecurity Act, and the AI Act (Renda, 2020, 2021).

→ To summarize, in the quest for European digital sovereignty, values are translated into regulations, which are then to be turned into protocols and interfaces (Renda, 2021). The EU is thus shifting from a status described by the adage "code is law" – where the technical architecture of the Internet determined the rules of behavior in the cyberspace and by extension cyberspace legislation – to "law is code," where Europe's chosen values and rules shape the technologies that are allowed in its market (Timmers, 2019, 2022b).

2.2 Cloud Computing

This thesis focuses on cloud computing through the lens of digital sovereignty. In simple terms, cloud computing can be understood as a combination of technologies allowing the delivery of computing power and related capabilities via the Internet, leading to significant savings on client IT infrastructure (McGillivray, 2022). This section outlines the most fundamental properties of cloud computing and a set of basic terms associated with the technology. Unlike digital sovereignty, cloud computing has a commonly agreed-upon definition, which is presented first. Next, three classification conventions within cloud computing are introduced – the main cloud computing parties, cloud service models, and cloud deployment models –,, and the global as well as European cloud market landscape is briefly reviewed. The final subsection delves into the role of cloud computing in the digital transformation of government organizations, considering the principal benefits and limitations of the technology from the perspective of the public sector.

2.2.1 Definition of Cloud Computing

The most widely accepted definition of cloud computing, referenced without any changes throughout the past decade (e.g., by McGillivray, 2022; Rosati & Lynn, 2020; and Zwattendorfer et al., 2013), was originally formulated by the U.S. National Institute of Standards and Technology (NIST). It reads: "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (…) that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell

& Grance, 2012, p. 2). The resources that are pooled include servers, storage equipment, networks, operating systems, software, or applications.

The International Organization for Standardization (ISO) defines cloud computing similarly – as a "paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand" (2014, p. 2). This definition encapsulates six key features of cloud computing:

- **Broad network access** from any location, promoting use by heterogenous client platforms and devices (ranging from workstations to mobile phones);
- **Measured service**, where usage is monitored so the customer is only billed for the resources they use;
- **Multi-tenancy**, where a set of physical or virtual resources might be made available to multiple customers, whose computations and data are isolated from and inaccessible to one another;
- **On-demand self-service**, where the provisioning of various types of computing capabilities requires no interaction between the customer and the cloud service provider;
- **Rapid elasticity and scalability**, where capabilities can be rapidly adjusted to quickly scale outward or inward in accordance with demand; and
- **Resource pooling**, where physical or virtual resources (i.e., storage, processing, memory, or network bandwidth) can be aggregated in order to efficiently serve multiple tenants, while using abstraction to mask the complexity of the process from the customer. (ISO, 2014; Mell & Grance, 2012; Nanos et al., 2019; Pearson, 2013)

2.2.2 Cloud Computing Classification

Many of the most common terms associated with cloud are in fact categories within three aspects of cloud computing – the roles played by different cloud computing parties and the different service and deployment models on offer. Echoing the language of digital sovereignty, the different possible service and deployment models entail different possibilities of distributing control over data and infrastructures, among the parties.

2.2.2.1 Cloud Computing Parties

There are three main types of parties involved in cloud computing business relationships:

- **Cloud service customers**, who use the cloud services (these may be companies or public sector organizations);

- **Cloud service providers (CSPs)**, who deliver cloud services to customers, which also entails cloud service maintenance and monitoring, security and business plan management, and the provision of audit data; and
- **Cloud service partners**, who act as intermediaries between the provider and the customer (ISO, 2014). There are two main types of cloud service partners – *cloud auditors* and *cloud brokers*. The role of auditors, typically performed by an independent third-party firm, is to examine if the cloud service provider complies with a standard certification scheme. Such audits are a critical point for the adoption of cloud services by governments. (McGillivray, 2022) Cloud brokers, also known as integrators, assist the customer with technical or business aspects of cloud computing adoption, which tend to be too complex for customers to manage themselves. Brokers help clients understand and customize the services on offer by the cloud providers, they manage the migration from clients' legacy systems into cloud services, and they may be able to obtain improved contract terms from the providers. Cloud brokers also sometimes provide cloud services on infrastructure they control. They may or may not have access to cloud client data. (Kuan Hon et al., 2012; McGillivray, 2022)

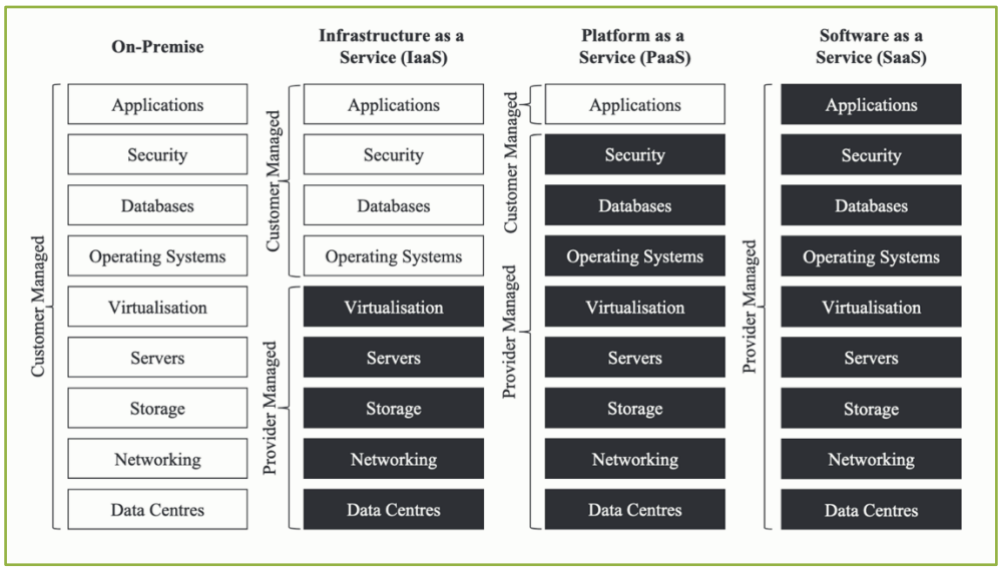
2.2.2.2 Cloud Service Models

Cloud infrastructure can be conceptualized as a combination of two layers: a physical layer, comprised of hardware resources – themselves often depicted as sub-layers – such as server, storage, and network components, and an abstraction layer, consisting of the software deployed across the physical layer (Mell & Grance, 2012)Depending on the customer's business requirements, different degrees of responsibility for and control over the cloud infrastructure can be exercised by the service provider, resulting in three main service models:

- **Infrastructure as a Service (IaaS)**, where the customer rents computing resources, such as processing power, storage, and networks, on a virtualized server. The provider thus takes over tasks related to maintaining a physical infrastructure and can quickly offer extra resources on demand. The customer preserves control over the software deployed on the cloud service, including the operating system, applications, and data stored on the cloud service. (McGillivray, 2022; Mell & Grance, 2012; Rosati & Lynn, 2020)
- **Platform as a Service (PaaS)**, where the customer is provided the capability to deploy, manage, and run customer-created or customer-acquired applications on the CSP's infrastructure. The customer can control the configuration settings for the application-hosting environment, using one or more supported programming languages. The aspects of the underlying infrastructure that fall under the provider's control are network, servers, operating systems, and storage. (ISO, 2014; Mell & Grance, 2012; Rosati & Lynn, 2020)

- **Software as a Service (SaaS)**, where the customer can access complete software solutions from a browser or a program interface on any Internet-connected device. All underlying cloud infrastructure – from the servers and operating system to storage and individual application capabilities – is managed and controlled by the cloud service provider. (Mell & Grance, 2012; Zwattendorfer et al., 2013)

Figure 2.1 below is a general cloud computing stack diagram, which compares the baseline, on-premise server architecture, with the three main cloud service models. On-premise environments (be they private clouds or traditional IT infrastructures) are fully operated by their owner, while in different cloud service models, some or all of the layers of the cloud stack are managed by the CSP. The diagram clearly shows how digital sovereignty diminishes as one moves from on-premise solutions through IaaS and PaaS to SaaS.



Source: Rosati and Lynn[17] (2020), p. 22

Figure 2.1 A cloud stack diagram comparing the three main service models

In recent years, with the proliferation of new IT architectural and business models, additional cloud service categories have emerged, many of which could however be subordinated to one of the three basic cloud service models from a technical perspective. According to McGillivray (2022), many of these models are "more aptly characterized as marketing achievements than technical ones" (p. 23). Collectively, such offerings are referred to as "XaaS" – Anything as a Service (sometimes also called Everything as a Service), where X can be replaced with any product that is delivered over a network. Examples include Data as a Service, Data Protection as a Service, Data Storage as a Service, Database as a Service, Network as a Service, Security as a Service, Compute as a Service,

[17] These authors did not invent the diagram – it originated in the private sector rather than in academia and its authorship is difficult to ascertain.

Communications as a Service, Logging as a Service, or Government as a Service. (ISO, 2014; McGillivray, 2022; Rosati & Lynn, 2020)

2.2.2.3 Cloud Deployment Models

There are four basic cloud computing deployment models, representing different ways to organize cloud computing based on the control and sharing of physical resources (ISO, 2014):

- **Private cloud**, where cloud services are used exclusively by a single organization, which also controls the resources (private data centers). In some cases, a private cloud may also be owned, managed, and operated by a third party and offered to the customer via the Internet or a private internal network. The cloud might be located on premises (of the organization) or off. (ISO, 2014; Turab et al., 2013) This model offers the most security, as it allows the client to exercise stricter boundary controls than other models. This deployment model best accommodates governments' strictest legal requirements related to jurisdictions and security (McGillivray, 2022).
- **Public cloud**, where cloud services owned and managed by the cloud service provider are made available over the Internet to any cloud service customer (provided jurisdictional regulations allow it). This model is optimal for customers seeking the highest value for money, as it allows customers to only pay for the CPU cycles, storage, or bandwidth they consume. (ISO, 2014; Nanos et al., 2019)
- **Community cloud**, where a cloud supports multiple organizations with shared characteristics (e.g., jurisdiction or industry) and concerns or needs (e.g., security requirements or compliance considerations). (Pearson, 2013; Turab et al., 2013) Such specific user requirements result in higher costs compared to public cloud, but lower compared to a private cloud. Community cloud may be managed by one of the organizations using it or by a third party. This deployment model is often used by public sector organization, such as the US GovCloud, which hosts a community of government agencies, all of which require that the cloud infrastructure be located in the U.S. and that only U.S. citizens or green card holders be allowed to access or handle the data on this cloud. (McGillivray, 2022; Tancock et al., 2013)
- **Hybrid cloud**, which is a composition of elements of two or more distinct cloud infrastructures (private, public, or community), bound together by standardized technology enabling data and application portability (Mell & Grance, 2012). Typically, hybrid clouds combine public and private clouds as a compromise between cost-saving and security considerations. This deployment model is becoming the standard among EU governments, which usually divide administrative data into several categories and keep

> the most sensitive data on private networks, while low-risk data are allowed to be stored in public clouds. (McGillivray, 2022)

Considering the benefits and drawbacks of the different deployment models, many customers opt for a multi-cloud strategy – the term *multi-cloud* refers to a cloud service customer's portfolio of cloud computing services offered by diverse providers, regardless of the deployment models involved, including using these different services simultaneously to execute one application (Ferrer et al., 2016). Similarly, customers may have a multi-vendor strategy to remain informed of the range of options on offer, maintain customer leverage, and prevent vendor lock-in (Moerel & Timmers, 2021).

In addition to the four main cloud deployment models, there are multiple types of *interconnected clouds*. Interconnected clouds are created by making several public (and private) clouds interoperable – in contrast to the spectrum of typically unineroperable proprietary cloud technologies that define the public cloud landscape (Altmann & Aryal, 2020). Interconnected clouds have the same cloud interfaces, allowing for seamless migration of virtual machines between clouds owned by different CSPs. Integration takes place at several levels, from agreed exchanged data formats to non-technical considerations such as compatible resource allocation policies (Esposito et al., 2016).

Altmann and Arval (2020) distinguish between two broad types of interconnected clouds. The first type is *interclouds*, where two or more clouds owned by a single provider are interlinked to increase the quality of service (e.g., to reduce latency). Interclouds can be public, private, or hybrid, depending on their composition. The second type is *federated clouds*, where clouds owned by multiple CSPs, are interconnected following a federation service level agreement for deploying standardized customer applications (Altmann & Aryal, 2020). One of the aims of the GAIA-X association is to create a federated European cloud by linking interested European CSPs together via a common architecture of regulatory and technical standards (Braud et al., 2021). In addition to the "standard" case of federated public clouds, Altmann and Arval (2020) further divide federated clouds into federated hybrid clouds (where a private cloud is given access to a group of interconnected public clouds for additional cloud services), federated hybrid interclouds (which only differ from the former in that the private cloud is an intercloud), and federated interclouds (where there is no private cloud).

Because federated clouds are the most complex deployment model and because it is the one underlying the European cloud federation and GAIA-X, their main benefits and challenges warrant elaboration. The benefits of cloud federation include increased scalability (which especially benefits smaller cloud providers, who thus gain access to extensive infrastructure resources), better ability to accommodate spikes in demand, and higher cost-effectiveness (especially when workloads are moved to regions where operating costs are lower). In addition, federated cloud infrastructures where computing and storage resources are geographically

widely distributed, provide better conditions for disaster recovery. (Altmann & Aryal, 2020; Esposito et al., 2016) The main challenges associated with federated cloud services are related to diminished control over the physical location of the outsourced data and computational activities – to achieve the highest possible resource utilization, the federation middleware may be set to automatically replicate and move data between different data centers, possibly located in different countries (Esposito et al., 2016). Esposito et al. emphasize that this often takes place without the data owner's consent, especially if the customer's data is in a federated public cloud and under a relatively weak service-level agreement, for example with regard to the localization of such "split" data (2016). On the other hand, strong geolocation restrictions on data storage and movement undermine the potential benefits of cloud federation and may still be circumvented by CSPs; hence, the authors stress the crucial role of encryption for data at rest in federated clouds (Esposito et al., 2016).

2.2.3 The Market Landscape

The potential of cloud computing is only truly realized when sufficient scale is achieved, which requires an amount of capital, know-how, and existing infrastructure that only the largest tech companies possess (Daly, 2016). The cloud market is thus highly concentrated – for example, as of the fourth quarter of 2021, four largest cloud service providers accounted for 70% of the global cloud infrastructure[18] market share (Amazon Web Services (AWS) held a 33% market share, Microsoft Azure 21%, Google Cloud 10% and Alibaba Cloud 6% – mostly restricted to the Chinese market) (Baltrusaitis, 2022; Sheikh, 2022; Zarkadakis, 2022). No European firms can match the best-in-class service offerings of these companies, making European businesses and governments largely dependent on U.S. CSPs (Moerel & Timmers, 2021; Sheikh, 2022). (That said, many smaller European CSPs just do not have sufficient market visibility (European Commission, 2020)). As a result, the market share of European cloud providers in the EU market fell from 26% in 2017 to 16% as of mid-2021, with Deutsche Telekom (the sixth largest market player in the EU with just a 2% market share), OVHcloud, and Orange being the largest players (Baltrusaitis, 2022; CEO Roundtable Members, 2021). The French market has the largest share of European CSPs, with OVHcloud and Orange taking the third and fourth position respectively, after AWS and Microsoft Azure (whereas in most of Europe, the third and fourth place are occupied by Google Cloud and IBM) (Baischew et al., 2020).

In addition to capitalizing on economies of scale, other ways in which the so-called hyperscalers have been able to maintain and expand their oligopolistic position (Glasze et al., 2022; Zarkadakis, 2022) is the trend of vertical integration, whereby they leverage their dominance from the cloud market into other markets (e.g., data analytics and AI, cybersecurity, or productivity software offerings) (Daly, 2016; Moerel & Timmers, 2021),

[18] The statistic covers PaaS, IaaS, and hosted private cloud services and is based on data by Statista

and the practice of systematically acquiring smaller rivals (Moerel & Timmers, 2021). Dominant CSPs also bind their customers to their products by erecting technical barriers to switching to other providers through the lack of interoperability, data portability, and data structure and application programming interface (API) standardization (Opara-Martins et al., 2016). However, as shown in subsection 3.1.4.3, recent EU legislation, especially the Data Act and the DMA, seeks to challenge such practices.

2.2.4 Public Sector Cloud Adoption

In the current "New Digital Era Governance" paradigm described by Tan and Crompvoets (2022), governments are adopting new digital technologies and tools to collect, store, and process data more economically, efficiently, and at a much larger scale than in the previous paradigm[19]. Applications of cloud computing are at the center of this process – in 2021, government use of public cloud services saw, according to an estimate by Gartner, a double-digit yearly growth rate (Tan & Crompvoets, 2022). Not only does using this technology save public sector organizations significant costs (which remains the main driver of cloud computing adoption among businesses and governments alike); it can also create public value, including by improving the quality, transparency, and innovativeness of public services and stimulating the data economy (Irion, 2012; Liang et al., 2019; McGillivray, 2022; Pearson, 2013; Tan & Crompvoets, 2022). However, the considerable benefits of cloud migration need to be weighed against the limitations, especially the diminished control over critical data – that is, potentially diminished digital or data sovereignty (Esposito et al., 2019; Irion, 2012). In this subsection, the possible benefits and limitations of cloud computing technology use by governments[20] are first listed separately and then discussed through the lens of a decision-making model used by EU public administrations.

Benefits. **(1)** By using cloud computing services, government organizations can spare themselves the need to invest taxpayer money in the construction or upgrading of their own data centers and to spend significant funds every month on operational expenses (from infrastructure maintenance to paying qualified IT personnel, whom the public sector tends to struggle attracting in the first place) (Al Ghaffar, 2020; Irion, 2012; Mohammed et al., 2016). As the legacy IT infrastructure of governments is rarely centralized, smaller or lower-level departments especially stand to gain from the ability to access powerful hardware and a diverse offering of affordable software that they would struggle to develop in-house (Irion, 2012; McGillivray, 2022; Mohammed et al., 2016). Relatedly, a single cloud-based solution can easily integrate the isolated IT systems of many otherwise administratively disjointed

[19] That is, in Digital-Era Governance of the 2000s, which, as described by Dunleavy et al. (2006), entailed reintegration of previously outsourced functions back into the governmental sphere. New Digital Era Governance's shift towards private CSPs speaks to the reversal of this process (Tan & Crompvoets, 2022).

[20] In this subsection, especially public, community, and hybrid cloud deployment models are being compared with both in-house IT departments and traditional IT outsourcing arrangements.

government departments and promote inter-agency collaboration (Carullo & Ernst, 2020; Liang et al., 2017, 2019). **(2)** In addition, clouds are usually more environmentally friendly than the alternatives (Almarabeh et al., 2016). The pay-as-you-go pricing model of clouds enables government organizations to only pay for the resources which have been consumed. This can be contrasted with the notoriously low server utilization in public sector organizations, which wastes both funds and electricity, thus leading to an unnecessarily high carbon footprint (Irion, 2012; Nanos et al., 2019; Zwattendorfer et al., 2013). **(3)** Government services or systems running on a cloud infrastructure are often of a higher quality than their previous incarnation was, especially in terms of speed and performance, remote accessibility (e.g., from any location and any device), and availability (with little to no downtime) (Abied et al., 2022; Nanos et al., 2019). This goes hand in hand with the increased efficiency and effectiveness of administrative processes and increased productivity of public servants. (Irion, 2012). In addition, the variety of modules and functions on offer encourages the development of innovative public services (e.g., the integration of participative elements) and the application of advanced Big Data analytics (Almarabeh et al., 2016). **(4)** Cloud-based services are very flexible – they are relatively simple to implement and easy for government staff to maintain (e.g., patches and updates are handled by the CSP). They are also elastic easily scalable, enabling institutions to cope with sudden increases (and subsequent decreases) in workloads by rapidly (automatically) provisioning and de-provisioning resources at peak demand times (Al Ghaffar, 2020; Catteddu, 2010; McGillivray, 2022; Zwattendorfer et al., 2013). **(5)** Another possible characteristic of cloud services is enhanced security compared to previous solutions, as CSPs have substantial resources available to solve security problems (Mohammed et al., 2016). **(6)** Backup and recovery of data is easier. Government services relying on cloud computing are thus more likely to maintain business continuity in the event of a disaster, e.g., one causing the breakdown of a data center – CSPs routinely use backup servers enabling disaster or ransomware recovery. (Abied et al., 2022; Almarabeh et al., 2016; Nanos et al., 2019). **(7)** Cloud computing can also help governments realize their transparency commitments, e.g., by supporting their open data portals (where public sector datasets with APIs are available for reuse) (Irion, 2012).

Limitations. (1) The main limitation of cloud computing is related to the reduced user control over data and consequently potential uncertainty surrounding data privacy and confidentiality (see also section 2.3.1). Regulatory compliance is especially difficult to ensure if the customer's data is stored in another jurisdiction with different data protection laws (Al Ghaffar, 2020; Nanos et al., 2019). From the customer's perspective, CSPs' approach to key information management issues is often rather opaque. For example, cloud vendors may have a policy of not specifying which security methods they use, their infrastructure is often dispersed across many undisclosed physical locations and countries (to achieve lower latency), and they may or may not use third party sub-providers (El-Gazzar et al., 2016; Jones et al., 2019; McGillivray, 2022; Scoon & Ko, 2016). (In the most extreme cases, government

employees with limited understanding of the risks associated with cloud computing services may, for example, inadvertently authorize a CSP to generate additional revenue from secondary use of the data (Catteddu, 2010; Pearson, 2013).) **(2)** Relatedly, traditional safeguards public institutions put in place to ensure information security and confidentiality of sensitive government data, such as regular on-side audits or non-disclosure agreements signed by each individual staff member with potential access, may not be applicable or available in the cloud computing environment. Facing pressure to quickly switch to the cloud, a government agency might not have the necessary cloud-specific processes and standards for managing data, architectures, and security in place by the time of cloud migration. (McGillivray, 2022; Paquette et al., 2010; Pearson, 2013) **(3)** Even when a government has the expertise and negotiating power[21] to secure favorable service level agreements (SLAs) from its CSPs (e.g., with data localization requirements), its data may still be exposed to grave security risks, especially if it resides on public, multi-tenant clouds (Esposito et al., 2019; McGillivray, 2022). Turab et al. (2013) list a range of possibilities for security attacks at the level of the CSP (e.g., an injection of an SQL command into a database or using a malicious insider working at the data center), network (e.g., domain hijacking and denial of service attacks), and end user (e.g., phishing). As evidenced by the famous "SolarWinds hack" of 2020 (which also exploited Microsoft and VMware products), attacks compromising the infrastructure of large-scale cloud providers to steal government data, are not just a theoretical risk (Marelli, 2022). According to the U.S intelligence community, the SolarWinds hack was a supply chain attack (and an act of cyber espionage) by a Russian state-sponsored group, whereby Orion, a software product for managing IT resources along business supply chains, was infected with malware, which created a backdoor to the data of six European Commission institutions and multiple U.S. government institutions including the Department of Defense, Treasury, and Homeland Security (Marelli, 2022). The consequences of such data breaches are devastating, especially in the case of extremely sensitive data types held by governments (e.g., census data, criminal records, or tax records) and politically strategic data (McGillivray, 2022). **(4)** Some cloud computing solutions may also suffer from operational issues such as poor performance, low service availability, (artificially) limited storage capacity, customization limitations, and disaster recovery restrictions (Jones et al., 2019). **(5)** Another danger is that of dependency on specific technologies or providers, which may lead to vendor lock-in (e.g., via file format lock-in), particularly in cloud-based SaaS solutions, with Microsoft Office 365 being a notorious example (Lundell et al., 2020; Zwattendorfer et al., 2013). Lack of interoperability and data portability as well as cloud providers' proprietary APIs also limit customers' ability to switch vendors (Nanos et al., 2019; Paquette et al., 2010).

[21] See Kuan Hon et al (2012), McGillivray (2022), and Wagle (2017) for a comprehensive discussion of the main issues where future customers push against standard terms in cloud (procurement) contracts – these issues include provider liability, termination rights, intellectual property rights, data protection requirements, or unilateral amendments to service features.

Government cloud technology adoption decision-making. For over a decade, public sector organizations across sectors and administrative levels have been facing the difficult task of weighing the benefits of different service and deployment models of cloud computing against the limitations to make an informed decision whether, or to what extent and under which conditions, they should adopt the technology. To simplify the complexity of this process, the European Network and Information Security Agency (ENISA) created a decision-making model in 2010, which European public sector organizations can use to identify the architectural solution that best suits their needs (Catteddu, 2010; Nanos et al., 2019). Because the model provides valuable insight into the best practices in European public sector IT and cybersecurity (and largely overlaps with, for example, the criteria for analyzing CPSs' SLAs applied by Wagle (2017) or McGillivray (2022)), it deserves to be outlined in some detail rather than just mentioned. The seven steps ENISA recommends undertaking when considering the implementation of a cloud solution, can be summarized as follows:

- First, the organization needs to define its operational, legal, and regulatory requirements. Here, the most important considerations are the types of data that would be stored by the CSP (i.e., personal, sensitive, classified, or aggregated data); the user profile (e.g., users' geographic distribution, level of security awareness, etc. – this pertains to both citizens and government employees); scalability and capacity management issues (e.g., whether traffic loads are expected to fluctuate widely); interface interoperability (e.g., whether the system will need to be able to exchange information with other systems, and if so, via which means of transfer, data formats, identity systems, etc.); the budget (with respect to the initial capital expenditure, cost of migration, and operational costs); and the ownership requirements (e.g., if the cloud must be owned and provided by the government or if it may be government-owned and third party operated, etc.). (Catteddu, 2010)
- Second, the required security and resilience parameters are to be identified, considering the whole service delivery supply chain (security refers mainly to the protection of data from unauthorized access and use; resilience describes a system's ability to function at an acceptable level in the face of challenges to normal operation). Here, the government organization needs to determine what risk analysis and assessment practices it wants the CSP to perform and how frequently; whether real-time security monitoring is required and what reporting requirements it will impose on the provider; how the efficiency of patch management is to be verified; whether the CSP is expected to allow the customer to access system logs; and whether and how partners in the service delivery supply chain will be audited (Catteddu, 2010). Also, the service providers' response and recovery strategy is to be evaluated (e.g., mean time to incident discovery or mean time to repair). In addition, legal and regulatory compliance needs to be enforced (including minimum and maximum data retention periods, confidentiality and other legal requirements, which may necessitate certain types of encryption etc.) (Catteddu, 2010)

- Third, all the possible architectural options are to be listed, ranging from non-cloud options (i.e., either in-house or outsourced IT infrastructures and services not based on cloud technology) to all the cloud service and deployment models (Catteddu, 2010).
- Fourth, a comparative risk assessment (or a SWOT analysis) is to be performed, in which each of the architectural options identified in step three is to be evaluated with respect to the operational, legal, and regulatory variables identified in step one and the security and resilience parameters discussed in step two. Based on this systematic comparison, the most suitable IT architecture is to be selected (Catteddu, 2010).
- Fifth, threats and weaknesses of the chosen solution are to be identified for each specific government service it will support (Catteddu, 2010).
- Sixth, a request for proposal is to be prepared to stipulate measures to minimize the threats and weaknesses identified in step five. These measures may be stated in the procurement criteria or in the contract. After that, a partner provider can be selected. (Catteddu, 2010)
- Seventh, informed by the threats and weaknesses from step five, a risk mitigation plan is to be created, which can be used in the risk treatment phase (Catteddu, 2010).

Following the definition of digital sovereignty formulated for the purposes of this thesis (see section 2.1.1), it can be said that the closer a government manages to get to implementing a cloud computing-based solution that satisfies all the best-case-scenario requirements and parameters defined in steps one and two, the closer it approaches digital sovereignty.

→ Organizations tend to converge on similar conclusions after applying decision-making models such as the one proposed by ENISA. In a compromise solution balancing the benefits of cloud computing with the limitations, public clouds are typically used for low-risk e-government applications and administrative systems involving non-sensitive data, while private and community cloud deployment models are chosen for more critical governmental services, as they offer greater control over the physical infrastructure and greater data security (El-Gazzar et al., 2016; Nanos et al., 2019; Zwattendorfer et al., 2013) – thus better safeguarding digital sovereignty. Nevertheless, the uptake of cloud computing in the European public sector is still low (European Commission, 2020).

2.3 European Digital Sovereignty and Government Cloud Computing

This section explores some of the ways in which the set of discourses and practices associated with European digital sovereignty intersects with the process of public sector cloud adoption in Europe. Recalling what is laid out in the previous sections of this literature review, the European model of digital sovereignty mobilizes relevant European values through regulations and standards, while digital sovereignty at the level of public sector organizations is understood as the ability to control citizen data and the infrastructures on

which they are stored and processed. Applied to the context of government cloud computing, there are several ways of upholding or exercising this control. Almost full control is achieved when trustworthy government employees implement and run a public sector organization's own private cloud (ideally located in a Cold War era bunker – see Taylor (2021)), capable of delivering excellent functionality combined with high cybersecurity standards. However, this is rarely an option (especially in the case of SaaS solutions) – most government organizations have to contract private CSPs and enforce this control through insisting on a set of key operational and security parameters in the procurement and contracting process. Now, many initiatives associated with European digital sovereignty ultimately strengthen individual public sector organizations' digital sovereignty by strengthening their leverage vis-à-vis the CSPs.

The following subsections discuss the most important of such initiatives. The first subsection defines the crux of the problem these initiatives are seeking to solve. As outlined in subsection 2.1.2, public sector organizations face three main types of threats to their digital sovereignty: the threat of powerlessness vis-à-vis specific CSPs, the threat of cyberattacks, and the threat of cyber espionage. While these are all pressing (and interrelated) threats, the European digital sovereignty policy debate in relation to cloud computing particularly emphasizes the last threat. Therefore, although all three threats are addressed in this section, the threat of cyber espionage is considered the core problem and receives the most attention. The second subsection focuses on initiatives whose impact can only be expected to unfold in the long term, as their goal is to reinforce the EU's digital sovereignty by focusing on its technological sovereignty in cloud computing, and on several key initiatives that can improve European public sector organizations' digital sovereignty in the short term, both through certification schemes and through intergovernmental cooperation. Crucially, a closer look at the initiatives in question reveals that there is hardly any consensus in the EU regarding the preferred ways of solving the problem of slipping digital sovereignty. In fact, the policy initiatives are being contested both among and within Member States, which hints at the fact that not all stakeholders in the EU subscribe to the European digital sovereignty narrative – including some of the supposed beneficiaries of certain European digital sovereignty measures. Some of the main points of contestation with regards to these initiatives are thus covered in the third subsection, to set the stage for the empirical part of this thesis, which explores this policy debate in depth.

2.3.1 The Core Problem: The Extraterritorial Reach of U.S. Law

In the near absence of domestic alternatives, EU public sector organizations have been contracting U.S. cloud service providers. However, such organizations have found it especially problematic to reconcile EU data protection requirements with three key pieces of U.S. legislation: the Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act (PATRIOT Act – now no longer in effect), the Foreign

Intelligence Surveillance Amendments Act (FISA Act), and the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (Christakis, 2020; De Filippi, 2013; Hildén, 2021).

The PATRIOT Act, which was passed in 2001 in the wake of the September 11 attacks, was the first U.S. law to be widely considered to conflict with European data privacy laws (De Filippi, 2013; Irion, 2012). The Act (which, after several extensions, expired in 2019) permitted U.S. authorities to require U.S.-based CSPs to disclose foreign individuals' personal data stored in or transmitted into the U.S. (Google publicly confirmed that it had been compelled to hand over EU citizens' data to U.S. intelligence agencies numerous times) (De Filippi, 2013; Irion, 2012). This prompted a series of legislative and institutional measures at both Member State and EU level to regulate the transfer of personal data beyond the European Economic Area, the increased awareness about 2000's Safe Harbor Privacy Principles[22] (whereby U.S. companies, including CSPs, were able to transfer EU citizens' data to the U.S. if they were able to, on a voluntary basis, offer a level of data protection similar to that granted by EU regulations), and the decision of many U.S. CSPs to offer their customers the option to confine their data to EU-based data centers (De Filippi, 2013; Scoon & Ko, 2016).

The FISA Act of 2008 grants the U.S. government the ability to monitor the in-transit communication and access the data of non-U.S. citizens "with the compelled assistance of an electronic communication service provider (…) in order to acquire foreign intelligence information" (U.S. Privacy and Civil Liberties Oversight Board, 2014, in McGillivray, 2022, p. 85) – even if they are located outside of the U.S., even without prior notice or consultation, and even without a warrant (which is necessary in relation to U.S. data subjects) (De Filippi, 2013). With regards to EU citizens' personal data passing through U.S. CSPs' clouds, the FISA Act is recognized as one of the major challenges[23] to data privacy and digital sovereignty (De Filippi, 2013).

The CLOUD Act was passed in 2018 in response to Microsoft Ireland's refusal to comply with a production order issued by a magistrate judge in the Southern District of New York in search for evidence concerning a drug-trafficking case (de Hert & Thumfart, 2021). The warrant requested Microsoft to turn over all emails associated with a specific customer

[22] The European Commission's Decision legitimizing the Safe Harbor Framework was invalidated by the Court of Justice of the EU in 2015, following the "Schrems I" case, where an Austrian citizen lodged a complaint regarding the level of protection of his data held by Facebook, considering the revelations about the activities of the NSA (Scoon & Ko, 2016). In 2020, "Schrems II" – another case with the same plaintiff – then annulled the so-called EU-U.S. Privacy Shield, the Commission's attempt at replacing the Safe Harbor. The Court of Justice of the EU ruled that data controllers and processors need to ensure that transatlantic data transfers are guaranteed a level of protection equivalent to that provided by the GDPR (McGillivray, 2022; Ruohonen, 2021).

[23] Another one would be Executive Order 12333, which, together with the FISA Act, enables the NSA to collect data on a large scale for foreign intelligence purposes (see also subsection 2.1.4.1 above); under the PRISM program, data is collected by compelling U.S.-based service providers including CSPs to provide it to the NSA/FBI/CIA, while the Upstream program compels telecommunications operators to assist the NSA only. (Hildén, 2021; McGillivray, 2022)

account, which were stored on cloud servers located in Ireland, and Microsoft's appeals reached the U.S. Supreme Court, which dropped the case when the US legislator intervened by passing the CLOUD Act (de Hert & Thumfart, 2021). The Act enables U.S. law enforcement authorities, if they obtain a warrant, to access data in the "possession, custody and control" of a U.S. corporation even if the data is physically located outside the U.S. territory – thus, European data localization laws do not ameliorate the risks (Celeste & Fabbrini, 2021, p. 3; Kushwaha et al., 2020). The Act clashes with Article 48 of the GDPR, which recognizes third country courts' warrants[24] requiring personal data disclosures by data controllers or processors, only on the basis of an international agreement – which is currently not in place between the U.S. and EU Member States[25] (Hildén, 2021). According to Ruohonen, the CLOUD Act effectively deprecated Europeans' "constitutional protections provided by a jurisdiction where the data is stored" (2021, p. 444).

2.3.2 Solutions, Policy Initiatives, and Member States' Cooperation

Long-term solutions. The long-term solutions to organizational-level threats to digital sovereignty have to do with strengthening Europe's own technological and industrial capacity to nurture home-grown alternatives to the hyperscalers (in other words, boosting the EU's technological sovereignty and strategic autonomy). One of the most relevant policy documents associated with European digital sovereignty is the Berlin Declaration on Digital Society and Value-Based Digital Government, signed at a ministerial meeting during the German Presidency of the Council of the EU in 2020. It calls on public authorities at all levels to follow seven "cornerstone principles of the digital sphere," one of which is "digital sovereignty and interoperability" (German Presidency of the Council of the EU, 2020, pp. 3–5). With regards to this principle, the Berlin Declaration states that governments "must ensure that all underlying digital components of ICT solutions (hardware, software, and services) meet European requirements" and that the right conditions must be created "for Europe to develop and deploy our own key digital capacities, including the deployment of secure cloud infrastructure and interoperable services that fully comply with European legal provisions and ethical values" (2020, p. 5). To achieve this, the Declaration calls for a strengthened interoperability framework (including the development of common standards and modular architectures) and for the public sector to use open-source software and to make its data and tools available for reuse, thus ensuring "Europe's global competitiveness and data sovereignty" (2020, p. 5). The concrete policy action steps for Member States to undertake by 2024 include joint work towards "agreements on requirements for technology providers and solutions in the

[24] Similarly to the U.S. CLOUD Act, China's National Intelligence Law, passed in 2017, also obliges Chinese corporations to comply with extraterritorial warrants (Celeste & Fabbrini, 2021).

[25] The EU-U.S. Agreement to facilitate cross border access to electronic evidence, a mutual legal assistance mechanism that could provide a more internationally legitimate pathway to acquiring forensic evidence (Irion, 2012), has been at the negotiating table since 2019; meanwhile, EU Member States only reached political agreement on the related e-Evidence Regulation proposal in November 2022 – four years after the European Commission proposed it. (Hildén, 2021)

public sector that are essential for digital sovereignty," while the European Commission (EC) and other EU institutions are called upon to establish the European Alliance on Industrial Data and Cloud, to build "the next generation of secure, resilient and energy-efficient cloud computing capacities in Europe" (German Presidency of the Council of the EU, 2020, pp. 12–13). The first working-level meeting of this Alliance took place in December 2021.

The creation of this Alliance had also been endorsed by the European Council and all EU Member States, both in October 2020. The latter endorsement formally launched the Alliance, in a declaration entitled "Building the next generation cloud for businesses and the public sector in the EU." In it, Member States, in cooperation with the EC, agree to develop the next generation EU cloud supply for EU businesses and the public sector, including by introducing an investment plan combining private, national, and EU efforts (including the Recovery and Resilience Facility). The Declaration envisions interconnecting "data processing and storage infrastructures across the EU territory," covering all architecture levels (as well as the edge) (EU Member States, 2020, pp. 4–5). Public sector cloud capacities are to be modernized by interconnecting existing government cloud capacities, to help public sector bodies "lead by example in the uptake of cloud," reduce their operating costs, and improve public service delivery (EU Member States, 2020, p. 5). With regards to the problems outlined in the previous subsection, the Declaration states the following:

> *"Cloud providers participating in European cloud federation should guarantee* ***European standards*** *in terms of security, data protection, consumer protection, data portability and energy efficiency and* ***contribute to European digital sovereignty****, while meeting diverse cloud user needs and ensuring competitiveness. They must provide adequate assurance and enable EU citizens,* ***public sector*** *and businesses to* ***maintain control*** *over strategic and sensitive data. In particular, while all cloud providers are welcome in European cloud federation,* ***the resulting cloud capacities should not be subject to laws of foreign jurisdictions. In case providers are subject to such laws, they should demonstrate that verified safeguards are in place in order to ensure that any access request to data of EU citizens, businesses and entities is compliant with EU Law.*** [emphasis added]"
>
> (EU Member States, 2020, p. 3)

The precise nature of these safeguards will be clarified in a forthcoming EU Cloud Rulebook[26], which is currently being developed by the European Commission.

As part of the European Data Strategy, the EC has also launched the European Open Science Cloud, a trusted data environment and infrastructure which will provide European scientists and businesses access to reusable research data; the EC will also invest €2 billion in a High Impact Project on European data spaces and federated cloud infrastructures (Celeste & Fabbrini, 2021;

[26] The Rulebook can arguably be viewed as an *unofficial* contribution to the Safe Harbor/Privacy Shield saga (see footnote No. 22 above). (The official continuation of the saga is the Trans-Atlantic Data Privacy Framework, informally referred to as Privacy Shield 2.0, on which the EU and the U.S. reached an agreement in principle in March 2022 (it is hoped to be finalized in 2023). (European Commission, 2022)

European Commission, 2020) A related long-term initiative, already mentioned above, is GAIA-X, an international non-profit association initiated by the governments of Germany and France in 2019. Its members are mostly (but not exclusively) European companies; the dominance of German and French industrial players is visible in the affiliations of the leaders of GAIA-X's three committees (the data spaces business committee is led by representatives of BMW and Siemens; the policy rules committee is headed by individuals from Volkswagen and OVHcloud; and the technical committee is led by the GAIA-X CTO and a representative of Atos) (Gaia-X, 2022). By interoperating the European cloud infrastructure (among other things, by developing the standards underpinning the next generation of European data infrastructure), GAIA-X promises to create a trusted ecosystem where enough data is made available for AI-driven innovation in the EU (Braud et al., 2021; Moerel & Timmers, 2021). Based on principles of sovereignty-by-design that give customers full control over their data (Moerel & Timmers, 2021), GAIA-X is the EU's flagship digital and data sovereignty project (Codagnone et al., 2021; Lambach & Oppermann, 2022).

Short-term solutions. The (partial) solutions that can be put in place in the short term have to do with international agreements (see footnotes No. 22 and 26) and regulatory measures and legislative directives (see also subsection 2.1.4.3). They also take the form of industry standards and certification schemes (which can impose requirements on CSPs that smaller public sector organizations may not be in a position to impose) and involve the exchange of experiences and government cloud best practices among Member States.

Among the most relevant EU-level regulatory measures and legislative directives are the Cybersecurity Act and the NIS Directive (see also subsection 2.1.4.3). The Cybersecurity Act was crucial in helping MSs improve their cybersecurity capabilities, among other things, by strengthening ENISA's mandate (to facilitate greater cybersecurity-related cooperation between MS, including operational coordination in case of cross-border cybersecurity incidents; see also below) (Roberts et al., 2021). National transpositions of the NIS Directive have aided efforts to strengthen harmonize national cybersecurity capabilities in the EU (Moerel & Timmers, 2021). Most importantly, they also required companies identified by governments as operators of essential services (which included many CSPs) to implement mandatory security and notification requirements – in essence requiring international companies to adopt EU standards on order to operate in the EU (Roberts et al., 2021). The Directive will be replaced by the NIS 2 Directive (on which political agreement was reached in May 2022), which further harmonizes cybersecurity risk management and incident reporting and requires MSs to adopt policies addressing the cybersecurity in the supply chains of their IT service providers (including CSPs and other providers of data storage and processing services). Importantly, the GDPR's standard contractual clauses (SCCs) are also a key resource that can be used in contracts involving personal data transfers between the EU and third countries (Hildén, 2021). Among other things, the SCCs cover

requirements for data importers to inform data exporters when they receive requests for disclosure from (in this case non-EU) government authorities (European Commission, 2022h).

At the international level, the ISO/IEC 27000-series is a well-established family of information security, privacy protection, and cybersecurity standards frequently used by private companies and government agencies alike. ISO/IEC 27017 is specifically relevant for relationships between cloud customers and CSPs, as it lays out commonly recognized guidelines for areas such as information security policies, human resource security, access control, cryptography, the modalities of cloud customers' monitoring activity, information security incident management, and processes to manage other special situations such as the dissolution of the CSP (ISO, 2015). Getting the ISO/IEC 27017 certification is considered the bare minimum CSPs can do to demonstrate their commitment to security standards. In addition, different certification frameworks for CSPs have been developed at the national level, most notably including the German Federal Office for Information Security's Cloud computing compliance controls catalogue (known as C5) and the SecNumCloud framework of the French National Agency for the Security of Information Systems. SecNumCloud especially emphasizes that CSPs' operations and data must be located within the EU (Kabelka, 2022).

However, in recent years, there has been a trend towards the harmonization of cloud certification schemes in the EU. First, the European Secure Cloud (ESCloud) label (with 15 core technical and organizational requirements related to data ownership, confidentiality, and privacy) was created in 2016 by the French and German agencies on the basis of C5 and SecNumCloud, and the working group has been gradually broadened beyond the bilateral level. Second, in 2015, ENISA had already launched a Cloud Certification Schemes Metaframework, mapping the security requirements of different European cloud certification schemes used in the public sector (including EU institutions). Third (and most notably for the remainder of this thesis), in accordance with the Cybersecurity Act, ENISA is developing a European Union Cybersecurity Certification Scheme for Cloud Services (EUCS), whose draft version[27] was published in 2020. ENISA's Ad Hoc Working Group, tasked with the preparation of the scheme, has been one of the main inter-Member State (but also public-private) expert fora shaping the technical underpinnings of an emerging consensus on European digital sovereignty in cloud. The EUCS, which is suitable for any type of cloud service, defines three sets of security requirements corresponding with three assurance levels: Basic (intended to minimize known basic risks of incidents), Substantial (minimizing risks of cyberattacks carried out by actors with limited skills and resources), and High (aimed at state-of-the-art cyberattacks by actors with significant skills and resources) (ENISA, 2020). The certification scheme, which is expected to be finalized in 2023, will be a useful tool for cloud service customers. In particular, it will empower public sector organizations to "make

[27] This work also builds on the Cloud Service Provider Certification Working Group's Recommendations for the implementation of the CSP Certification scheme, published in 2019.

informed choices about the procurement and operation of cloud services" and to "allow regulatory authorities to refer to the scheme in European and national regulations" (ENISA, 2020, p. 12).

Other working groups have been instrumental in the spread of critical information among European public sector organizations. The NIS Directive established the NIS Cooperation Group for cross-border strategic cooperation and exchange of good practices between MSs, the EC, and ENISA on network and information systems security issues[28]. ENISA's own teams also performed extremely useful investigations with the help of IT officers from MSs, such as the Survey and analysis of security parameters in cloud SLAs across the European public sector. In 2013, ENISA, together with its Cloud Security and Resilience Expert Group, published a guide for securely deploying cloud services in the European public sector (Haeberlen et al., 2013). The publication reports on the state of the art among EU Member States (MSs) at the time and presented a set of recommendations for the EC and MSs, such as the recommended features of an EU strategy to foster the adoption of government cloud.

Besides working groups convened by ENISA, which facilitate capacity building, operational support, and standardization (Roberts et al., 2021), another important forum for exchange of best practices and pan-European policy coordination among national cloud experts is the informal Member States' Cloud Cooperation Group (MSCCG) of the European Alliance for Industrial Data, Edge and Cloud. The "actual" Cloud Alliance consists of industry representatives (from both the cloud-edge continuum and the aeronautics and defense industries), Member State representatives, and officials from the EC's Directorate-General for Communications Networks, Content and Technology (DG CNECT), and meets to discuss long-term measures largely related to building up Europe's technological sovereignty. In contrast, the MSCCG is a forum where MSs and DG CNECT representatives openly discuss and, where feasible, informally coordinate European governments' approach to cloud computing, largely based on national cloud policies.

→ As such, this group is the main policy venue in which EU and MS-level stakeholders debate policy issues at the intersection of European digital sovereignty and government cloud computing. Therefore, the work of the MSCCG is of key interest to the empirical section of this thesis, which draws on interviews with no fewer than four of its members.

2.3.3 Debates about the Solutions and Member States' Varying Positions

Debates about the long-term solutions. The academic literature covers numerous points of tension and contestation in relation to the above long-term initiatives and alliances. A commonly raised argument is that the planned investment in semiconductor technologies, supercomputing,

[28] The subjects on which the group has worked include cybersecurity of election technology, formats and procedures of digital service providers incidents, or a toolbox of risk mitigating measures for 5G networks.

AI technologies, and cloud data centers "still pales compared to the EU's economic competitors" such as the U.S. and China, leading to calls for the allocation of more public and private funds (Roberts et al., 2021, pp. 15–16). In a report addressed to the European Commissioner for the Internal Market, members of the CEO Roundtable "Shaping the Next Generation Cloud Supply for Europe" state that the technology priorities for the years 2021-2025 amount to a combined private-public investment need of €19 billion, with multiple areas – such as European cloud service standards, innovative data encryption technologies (including quantum safe encryption), increased density of edge facilities, pan-European data sharing platforms, and cloud native software for computationally intensive tasks on edge nodes – requiring predominantly public contributions (2021, p. 73).

Next, some scholars claim that the GAIA-X initiative will not do much to improve the position of European technology companies given that international hyperscalers are also welcome among the ranks of the association (Roberts et al., 2021; Sheikh, 2022) – as of November 2022, GAIA-X's 360 members[29] include Oracle U.S., Salesforce U.S., the Irish subsidiaries of Google and VMware, Microsoft Belgium, Amazon Luxembourg, Huawei Germany, and Alibaba Singapore (GAIA-X, 2022). On the other hand, some voices critique the above European digital sovereignty initiatives as "techno-nationalism" and "creeping protectionism" and warn that using national security as an excuse to unfairly discriminate against foreign players might backfire and "reduce, instead of increase, Europe's attractiveness in the digital sector" (Christakis, 2020, p. 52).

Debates about the short-term solutions. For similar reasons, ENISA's candidate EUCS and its data localization requirements have likewise attracted a large amount of controversy – many believe the digital sovereignty rhetoric is employed to unfairly discriminate against non-European market players. It is claimed that the assurance level High includes "sovereignty requirements" that disqualify CSPs that are not headquartered in the EU or that are in any way controlled by a non-EU entity (which, according to some accounts, might even apply to companies with a large share of foreign investors) (Bertuzzi, 2022; Kabelka, 2022). For the assurance level Basic, the candidate scheme requires CSPs to provide information "on the cloud service's jurisdiction and locations from a legal and regulatory perspective"; to be able to obtain certification for level Substantial, the CSP needs to also provide information about "the locations from which administration and supervision may be carried out on the cloud service" as well as all the locations where "any cloud customer data, meta-data or derived data may be transferred, processed, or stored"; and any CSP at assurance level High needs to also "document the locations from which it conducts operations for clients" and list such client support operations for each location (ENISA, 2020, p. 151). Scores of industry representatives have accused ENISA of allowing these

[29] In contrast, European Alliance for Industrial Data, Edge and Cloud has 51 member companies as of November 2022, all European.

supposedly technical and security-driven requirements to become political tools. In June 2022, ENISA and the EC received several open letters condemning EUCS's "sovereignty requirements." One of them was drafted by DIGITALEUROPE, which, through 41 national-level trade associations, represents over 45 thousand companies (in addition to 100 global corporations). DIGITALEUROPE's letter argues that the proposed requirements aiming to make EU data 'immune' from non-EU laws, in fact "fundamentally misunderstand the reality of European businesses operating internationally" and threaten to have the counterproductive consequence of restricting the choice and quality in the EU cloud market, while also hampering the global competitiveness of European companies, as no CSP with the "assurance level High" certification will be able to offer data transfers to third countries (DIGITALEUROPE, 2022, p. 1). Another open letter was written by several U.S.-based industry associations, which also expressed their concerns over the "potential inclusion of unhelpful 'digital sovereignty' requirements" localizing data storage, operations, and maintenance, as they would limit global CSPs' eligibility to the EUCS, thus limiting competition in the market, raising costs, reducing innovation, and creating obstacles to information sharing between organizations and paradoxically increasing cybersecurity risks (Information Technology Industry Council, 2022, p. 1; Swire & Kennedy-Mayo, 2022). The letter also claims that several (further unspecified) EU MSs would prefer to discuss and "clarify a common position on sovereignty at the political level" instead of through the EUCS (Information Technology Industry Council, 2022, p. 2).

Some of the arguments of the industry are echoed in the academic literature. First, localized data may indeed be *less* secure rather than more secure. Localized servers are more likely to act as a single point of failure than data centers spread across the globe – for example as a tempting target for criminals or foreign adversaries (Baezner, 2018; R. D. Taylor, 2020). Relatedly, Swire and Kennedy-Mayo (2022, p. 14) argue that data localization laws often create barriers to "integrated management of cybersecurity risk" within individual organizations including government agencies (e.g., by making impossible the use of offshore customer/user support centers). Second, while data localization policies can undoubtedly create a nurturing environment for the development of domestic technological capacity, when they do, they by definition amount to protectionist measures that challenge the global liberal economic order (Ruohonen, 2021; R. D. Taylor, 2020). Third, European data localization laws also contribute to the fragmentation (or "Balkanization") of the Internet (de Hert & Thumfart, 2021) – not unlike the Russian Sovereign Internet legislation (Epifanova, 2020). Furthermore, data localization rules are argued to disproportionately benefit larger CSPs, who are more likely to have the necessary resources to comply with the regulatory requirements, at the expense of SMEs; this also erects a barrier to market entry to potential innovators (R. D. Taylor, 2020). Finally, Taylor (2020) and Roberts et al. (2021) also discuss the tensions between data localization laws and trans-border data flows policies.

Finally, Hildén points out the fundamental contradiction between the measures recommended in the EC's SCCs for data transfers to third countries, and the European Data Protection Board's conclusion that "no contractual, organizational, or technical measures" can help any U.S. SaaS solution fulfill the conditions of Schrems II (see footnote No. 22 above), as the provision of SaaS requires momentary access to unencrypted data (2021, p. 8).

Variance among Member States. Different Member States' positions and progress on the above European digital sovereignty initiatives can be gleaned, for example, from the Report on the monitoring of the Berlin Declaration[30] (European Commission, 2022g). As part of this work, the Declaration's seven principles (associated with 22 policy actions) were assigned a total of 44 key performance indicators (KPIs), where KPI 29[31], labelled "participation of Member States in EU Actions essential for digital sovereignty," is most relevant (European Commission, 2022g). The two "actions" the monitoring survey asked about are the Industrial Alliance for Processors and Semiconductor Technologies and the GAIA-X Alliance (curiously, the European Alliance on Industrial Data and Cloud was not inquired about), and Member States had the option of selecting that they are part of the alliance, that involvement is under evaluation, or that involvement is not planned. The variance in Member States' results in this KPI is unsurprising – while, for example, France, Germany, Belgium, Finland, or Italy achieved a perfect score (100%), smaller countries tended to perform lower – e.g., Hungary, the Czech Republic, Sweden, or Latvia scored 50%, as they often selected "not applicable" in the case of the Processors and Semiconductors Alliance and "under evaluation" in the case of GAIA-X. This contributed to the fact that newer Member States tended to score below the EU average (78%) in the digital sovereignty policy area overall (which consisted of three KPIs) – Germany achieved a digital sovereignty score of 96%, Spain 97%, and France 81%, while the Czech Republic's result was 75%, Latvia's 58%, and Romania's 50% (of course there are outliers – for example, Croatia's overall digital sovereignty score is 92% and the country is highlighted in the report as being especially strong on KPI 29) (European Commission, 2022g).

Member States were also able to add comments, where most respondents listed the companies through which the country was represented in each alliance. Yet, the Czech Republic – one of the case sub-units of this thesis – gave a more reserved response regarding these alliances and suggested a different interpretation of digital sovereignty, one framed in terms of the elimination of vendor lock-in: "Both EU initiatives are being carefully evaluated at government level and in cooperation with the private sector. These are considered long-term projects with opportunities,

[30] This report was prepared by the French Presidency of the Council of the EU on behalf of the European Commission's Directorate General for Informatics (DG DIGIT). It is based on the Berlin Declaration monitoring exercise led by the EC's National Interoperability Framework Observatory.

[31] Corresponding with the policy action "Jointly work towards agreements on requirements for technology providers and solutions in the public sector that are essential for digital sovereignty" (European Commission, 2022g)

risks, costs and benefits. At the national level, minimizing the vendor lock-in situations in public administration are government priority" (European Commission, 2022, personal correspondence[32]). Such language evidences the varying attitudes among Member States towards the current direction of the European digital sovereignty agenda.

Source: Baischew et al. (2020), p. 19

Figure 2.2 Member States with a proactive or reactive approach to digital sovereignty

The above results correspond with the conclusions of Baischew and colleagues' (2020) benchmarking exercise on digital sovereignty in Europe, which divides Member States (and the UK) into those with a *proactive* and those with a *reactive* attitude to digital sovereignty[33] (see Figure 2.2). Countries taking a proactive approach recognize the cybersecurity and privacy aspects of digital sovereignty, but also take extensive geostrategic or economic policy measures to reduce dependency on non-EU providers (including CSPs), notably by pushing for the development of European alternatives (Baischew et al., 2020). The most proactive countries are France and Germany (Kushwaha et al., 2020), but also for example Estonia (with its invention of data embassies) or Denmark (with its Silicon Valley

[32] The breakdown of Member States' scores as well as their comments were obtained via personal correspondence with DG DIGIT and the consulting firm that was contracted to perform the monitoring exercise (Wavestone). The publicly accessible report also does not specify the "EU actions" that are essential for digital sovereignty.

[33] It should be noted that Baischew and colleagues' (2020) report is not a peer-reviewed publication.

"TechPlomacy"). Member States with a predominantly reactive approach prefer to "refrain from economic policy measures with a high degree of intervention," do not shy away from contract-based cooperation with U.S. CSPs, and interpret digital sovereignty almost exclusively as the need to put in place strong data privacy and cybersecurity measures. Newer Member States (including the Czech Republic) tend to be more reactive. (Baischew et al., 2020, p. 18; Kushwaha et al., 2020).

According to Baischew et al. (2020), while most EU countries seem to agree that Chinese suppliers should be carefully screened (or even partially restricted in the provision of 5G infrastructures), the main difference in proactive versus reactive countries' attitudes lies in their positions towards U.S. companies (including CSPs). The proactive countries, especially Germany and France (but not Estonia, Poland, and the UK) view U.S. suppliers, if anything, as a temporary solution until European firms become more competitive, while the reactive countries treat U.S. companies with a "softer attitude" – in fact, they tend to have bilateral agreements with the U.S. government on digital sovereignty issues such as selection criteria for 5G suppliers (as, for example, the Czech Republic does) (Baischew et al., 2020, p. 20). Kabelka (2022) highlights the same line of division in the digital sovereignty debate: France (always) and other large MSs (often) argue for emancipation from American technology by building up "European champions," whereas smaller MSs are reluctant to give up the best-in-class technology for the sake of helping French and German firms scale up.

→ One of the research motivations of this thesis is thus to explore the potential tensions between the proactive and reactive countries in the European digital sovereignty debate, which is why France and the Czech Republic were chosen as case sub-units, representative of the opposing sides.

2.4 Gap in the Literature

This thesis is a contribution to the literature exploring European digital sovereignty as a strategy to safeguard EU citizens' government-held data in the face of serious threats such as cyberattacks and cyber espionage. It builds on a strong body of previous work. The academic discussion about cloud computing's "inherent data sovereignty problem" (p. 66) and the possible remedies such as international and regional standard setting and "the harnessing of collective public sector buying power" was largely started by Irion (2012). Many subsequent articles (e.g., Couture & Toupin, 2019; Floridi, 2020; Ruohonen, 2021) develop Irion's theoretical analysis of the meaning of sovereignty with regards to data; others (e.g., De Filippi, 2013; de Hert & Thumfart, 2021; Gstrein & Zwitter, 2021; Hildén, 2021; Roberts et al., 2021; R. D. Taylor, 2020) build on her legal analysis of the role of multilateral regulation of (government) cloud services. Nevertheless, there has been limited follow-up on her calls for further research on this subject incorporating the

perspective of government officials and employees – yet, their perspective can provide valuable insight on the political tractability and technological feasibility of the European digital sovereignty policies in different national and organizational contexts (Irion, 2012).

In addition, very little academic work has focused on the ongoing debate among the Member States *and* EU institutions regarding the preferred future course of action in European digital sovereignty (in relation to cloud computing). Given that the "quest for digital self-determination" is the "central geopolitical issue" of this decade (Musiani, 2022), the latest developments in the debate shaping the block's coordinated policy are of crucial interest to all Europeans, whose data are at stake. Yet, the literature has mostly either focused on the EU level only (such as Roberts et al., 2021) or considered different national positions separately, typically highlighting France and Germany as leaders in the European digital sovereignty discourse (e.g., Kushwaha et al., 2020; Lambach & Oppermann, 2022), or focusing on, for example, the Dutch or the Swedish national experience (e.g., Hildén, 2021; Moerel & Timmers, 2021). This thesis aims to fill this gap by covering the coalitions formed by different Member State and organizational-level actors in the debate on European digital sovereignty and cloud computing, their respective concerns, and the expected results of their cooperation efforts under the auspices of the European Commission.

3 Conceptual Framework

The conceptual framework used in this thesis is the Advocacy Coalition Framework (ACF) – one of the most comprehensive and widely used conceptual frameworks for understanding and explaining policy processes (Brooks, 2018; Cairney, 2014; Radaelli, 1999; Weible & Sabatier, 2006; Yun, 2019). The ACF was chosen because it highlights the fact that like-minded policy actors act in a coordinated manner to achieve their policy goals, which was observed during the initial set of open interviews. The choice to split EU Member States into proactive and reactive groups also called for a framework that includes a mechanism for explaining varying policy preferences. Another reason why the framework was deemed suitable for this thesis is its universal applicability – as there is no body of literature on the subject of European coordination of national cloud computing strategies, it appeared to be a good idea to make a safe choice and select a commonly used framework to give the thesis a structure with which readers are familiar.

Since it was first proposed by Paul Sabatier in 1988, the framework has been revised and expanded several times. While the original version of the framework largely focused on policy-oriented learning and policy change in the US context (Sabatier, 1988), subsequent elaborations introduced a host of additional use cases, including EU-level policymaking (Sabatier, 1998). In this thesis, the most recent version of the framework, created in 2007 (Cairney, 2014; Sabatier & Weible, 2007; Weible et al., 2009), will be used; nevertheless, earlier sources will also be referred to when describing those aspects of the framework that have remained unchanged.

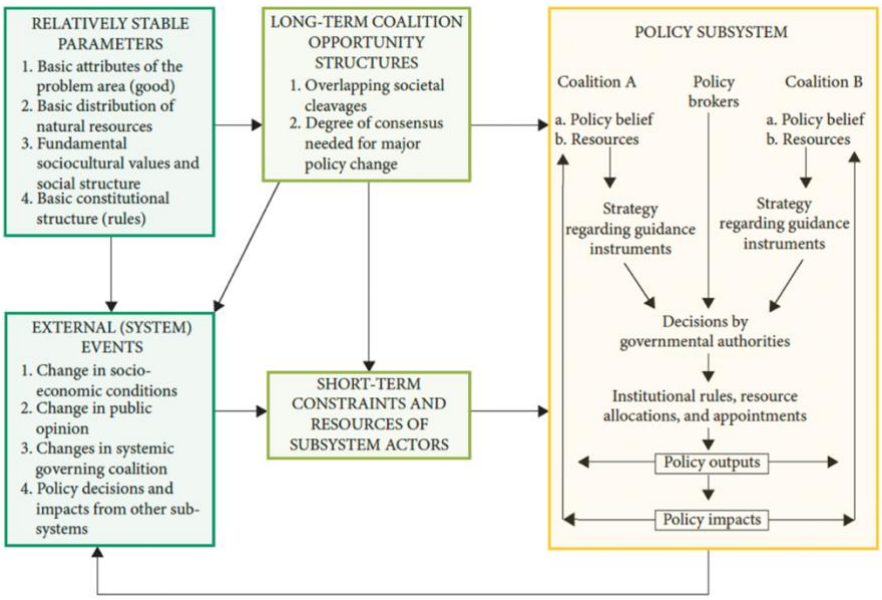
This chapter consists of two sections. In the first one, the ACF is introduced, and its components are described; in the second one, the literature informing the application of the framework is reviewed, and several decisions regarding the methodology and scope of this research are outlined.

3.1 Description of the Advocacy Coalition Framework

The ACF's logic rests on six key assumptions: (i) the central role of scientific and technical information in the policy process, whose interpretation and application is marked by considerable uncertainty (this firs the context of cybersecurity well – for example, different interviewees had different opinions on the degree to which two-way encryption can in fact be considered secure enough); (ii) the unsuitability of the short-term perspective in analyzing policy change – ACF's proponents reject the policy cycle heuristic for its lack of an underlying causal theory (this seems to fit the rather technical subject of government cloud policy well, as this is not generally a subject discussed during elections); (iii) the role of policy subsystems as the primary focal point of policy analysis; (iv) the necessity of inclusion of a wide cast of policy actors in the analysis – beyond elected representatives and lobbyists, there

are also "bottom-up" actors such as officials across government agencies and administrative levels, consultants, researchers, members of the media, and vocal actors from other countries (the role of non-politicians was confirmed by the interviewees); (v) the assumption that individuals are boundedly rational and likely to perceive and simplify the world through the lens of their preexisting beliefs, while dissonant information is screened out; and (vi) the view of policies as translations of beliefs, rather than merely of individual material interests. (Cairney, 2014; Sabatier, 1988, 1998; Weible et al., 2009; Weible & Sabatier, 2009)

The relationships between the ACF's overarching components are depicted in the ACF Flow Diagram (see Figure 3.1 below). The right side of the diagram displays the most basic component of the framework, the *policy subsystem*, which is defined as the set of actors or policy participants "involved in dealing with a policy problem" (Sabatier, 1988, p. 138) or a substantive issue, usually within a specific geographic boundary (Weible & Sabatier, 2009). In the case of this thesis, the policy subsystem of interest refers to all actors involved in the formulation of, implementation of, and discussion about public sector cloud policy. The term *policy participants* is not limited to political elites – it encompasses all actors attempting to influence subsystem affairs, be it directly or indirectly, including lower-level government employees involved in policy implementation and societal actors who are latent supporters of a certain policy and may only become active under specific circumstances (Sabatier, 1988; Weible & Sabatier, 2009). While the empirical part of this thesis does not explicitly address all the components of the framework, they do implicitly underpin the logic of the way in which the findings are presented. Therefore, for readers to understand the presented findings, it seems advisable to describe the ACF in detail.



Source: Cairney (2014), p. 487

Figure 3.1 The ACF Flow Diagram (2007 version)

Each policy subsystem consists of three main types of entities. Firstly, there are usually two or more competing *advocacy coalitions* (in some cases there may only be one; one powerful coalition often dominates multi-coalition scenarios for long periods). An advocacy coalition is defined as an aggregation of policy participants who share a particular belief system – i.e., values, "causal assumptions, and problem perceptions" – and who show a "non-trivial degree of coordinated activity" aiming to translate these beliefs into policy decisions and outcomes (Cairney, 2014; Sabatier, 1988, p. 139). In other words, beliefs are a causal driver of coalitions' efforts to influence policy (Weible et al., 2009). Models paying attention to advocacy coalitions in policy environments are argued to be superior to models that view formal institutions as the dominant actors, especially since the latter fail to account for the variation in beliefs and behavior among individuals and groups within the same institution (Sabatier, 1988). (Therefore, the EC, for example, was not treated as a homogeneous entity in this thesis.) The second entity in a policy subsystem is the *policy broker*, who is tasked with reaching reasonable solutions to problems by mediating and minimizing conflict between coalitions and producing workable compromises (Cairney, 2014). Policy brokers are usually trusted by both (or all) coalitions and enjoy some decision-making authority (Weible & Sabatier, 2006). The third entity is a *governmental authority* that makes policy decisions and oversees the policymaking infrastructure. Sometimes, the distinction between coalitions, brokers, and governmental authorities may be blurred – for example, a high civil servant might be both a broker and a policy advocate (Cairney, 2014; Sabatier, 1988). Policy subsystems can generally be described as either adversarial, or collaborative (Weible & Sabatier, 2009).

As can be seen in the flow diagram, actors forming a coalition (a) share the same policy beliefs (which then determine the direction of their advocacy efforts) and (b) use the resources available to them to improve their coalition's position within the policy subsystem (and their success will largely depend upon these resources) (Cairney, 2014; Sabatier, 1988). (a) To better understand the beliefs uniting members of the same advocacy coalition, the ACF introduces a three-tiered belief system hierarchy (not represented in the flow diagram). (i) *Deep core beliefs* are the broadest (also described as personal philosophies), most stable, and predominantly normative (examples include beliefs on whether offenders are redeemable). (ii) *Policy core beliefs* can be seen as fundamental, generally stable policy positions that have a moderate enough scope to guide policy-specific behavior – it is this type of policy belief that typically inspires the formation of an advocacy coalition (beliefs in this category may relate, for example, to the proper amount of government interference in market dynamics). (iii) *Secondary beliefs* (or *aspects*) are the narrowest in scope, more empirically based, and most likely to change over time (they relate to the practical details of policy implementation). (Cairney, 2014; Weible et al., 2009) The ACF expects actors within an advocacy coalition to show substantial consensus on issues stemming from their policy core beliefs, while at times disagreeing on the secondary aspects (Sabatier, 1988).

Policy core beliefs and secondary beliefs were used in this thesis as the most fundamental way of defining coalitions. (b) The policy-relevant resources coalitions leverage include formal legal decision-making authority, the weight of public opinion and support, funding, the composition of their membership, skillful leadership, and informational resources (Cairney, 2014; Sabatier, 1988; Sabatier & Weible, 2007).

Sabatier (1998) further describes the typical sequence of events within the policy subsystem as follows. In an effort to realize its objectives, each coalition adopts one or more strategies using *guidance instruments*, i.e., "changes in rules, budgets, personnel, or information" (Sabatier, 1998, p. 104). Coalitions seek to influence policy or other actors' beliefs in as many *venues* as possible (Weible & Sabatier, 2006). In the case of this thesis, the focus is only on one venue. With the help of a policy broker, coalitions negotiate and find a compromise solution; alternatively, one coalition's position prevails. Resultantly, a *decision by a governmental authority* is made regarding a change in *institutional rules, resource allocations, or appointments* (Knutsson, 2017). This decision produces a certain *policy output*, which then has a variety of *policy impacts*, including unintended consequences and side effects (Sabatier, 1998). Finally, policy outputs and impacts are considered and analyzed by each advocacy coalition; this might lead to a reevaluation of policy participants' secondary beliefs or to a revision of coalition strategies (Knutsson, 2017; Sabatier, 1998).

The left side of the flow diagram shows two sets of variables that are exogenous to a policy subsystem – one more stable, the other more dynamic – that provide each advocacy coalition with different opportunities and constraints (Cairney, 2014; Sabatier, 1998). There are four *relatively stable parameters:* (1) basic attributes of the problem area or good (such as a problem's susceptibility to quantitative measurement); (2) basic distribution of natural resources (e.g., the availability of oil reserves in a country); (3) fundamental socio-cultural values and social structure (e.g., whether nationalization of energy suppliers is a viable policy option in a given country); and (4) basic constitutional structure (which includes the constitutional framework, as well as for example the fundamental norms of administrative law). These parameters structure the nature of the policy problem and establish the rules and procedures for political decision-making and policy change. While they significantly affect coalitions' behavior, relatively stable parameters rarely play a large role in coalitions' strategies as they are resistant to change. (Sabatier, 1988, 1998; Weible & Sabatier, 2006)

The second box on the left-hand side lists possible external events that can alter the constraints and opportunities faced by the actors of a policy subsystem. *External system events* are the most dynamic elements of the ACF; as such, they are most likely to contribute to policy change. (Sabatier, 1988) There are four types of such events: (1) change in socioeconomic conditions and technology (e.g., economic dislocations causing the rise of social movements); (2) change in public opinion (e.g., regarding the relative seriousness of different problems); (3) change in systemic governing coalition (usually after an election); and (4) policy decisions

and impacts from other policy subsystems (e.g., unintended consequences of changes in tax policy on innovation). (Sabatier, 1988, 1998) These "boxes" are only considered implicitly in this thesis.

Lastly, the variables in the two boxes in the middle section of the flow diagram, which were introduced in the 2007 revision of the ACF (Sabatier & Weible, 2007), mediate the relationship between the stable parameters and external events on the one hand, and policy subsystems on the other (Yun, 2019). *Long-term coalition opportunity structures* refer to the nature of the political system in which the policy subsystem is nested (Cairney, 2014), namely (1) the overlapping societal cleavages (i.e., the degree of societal conflict) and (2) the degree of consensus needed for major policy change (i.e., the "number of people, organizations, and/or votes necessary to change existing policies") (Yun, 2019, p. 19). (In addition, more recent versions of the ACF also discuss the degree of openness of the political system (e.g., see Pierce et al., 2020; Sabatier & Weible, 2007).) *Short-term constraints and resources of subsystem actors* are then directly affected by both external system events and long-term coalition opportunity structures (Cairney, 2014; Yun, 2019). These variables are referenced in the discussion section.

The primary purpose of the ACF is to explain policy change over a long period (Sabatier & Weible, 2007). Thus, the framework recognizes four possible *paths to policy change* (Knutsson, 2017; Weible et al., 2009; Yun, 2019)*:* (i) policy-oriented learning, (ii) external shocks, (iii) internal shocks, and (iv) negotiated agreement. (i) A coalition may engage on *policy-oriented learning* (also referred to simply as policy learning), whereby it modifies its secondary beliefs in light of new information, often bringing them closer to the beliefs of another coalition. New evidence is always interpreted through the lens of core policy beliefs. (Cairney, 2014) Still, policy-oriented learning may result in alterations in behavioral intentions or a revision in a coalition's policy objectives (Weible et al., 2009). (ii) *External shocks* are triggered by major events such as disasters or crises, which bring considerable public attention to the policy problem and might shift or augment resources. If an advocacy coalition is successful at exploiting an external shock by convincing the public that its belief system renders it best equipped to understand and solve the policy problem, it can reinforce its position within the policy subsystem and effect policy change. (Cairney, 2014; Weible et al., 2009; Yun, 2019) (iii) *Internal shocks* also originate outside the policy subsystem but have significant effects on internal subsystem practices by highlighting their flaws (Weible et al., 2009). They occur when a major event challenges the policy core beliefs of many actors within a coalition, often causing them to join another coalition (Cairney, 2014). (iv) In situations where all major coalitions view a continuation of the status quo as unacceptable, they may reach *negotiated agreement* by finding a compromise solution, typically facilitated by a relatively neutral policy broker (Sabatier, 1988; Sabatier & Weible, 2007). In addition to such a "hurting stalemate," conditions increasing the likelihood of

policy change via the fourth path also include effective leadership, consensus-based decision rules, or a focus on empirical issues (Weible et al., 2009, p. 132).

3.2 Approach for Applying the Advocacy Coalition Framework

To devise a suitable approach for applying the ACF to the case investigated in this thesis, three types of sources were consulted: the methodological instructions by the authors and early proponents of the ACF (see subsection 3.2.1); reviews of the trends in past applications of the ACF (3.2.2); and a set of studies using the framework in the context of EU-level policymaking (3.3.3). This was judged to be an important step, as researchers frequently apply the ACF in ways that betray their oblivion to fundamental aspects of the framework (Jang et al., 2016; Weible et al., 2009), which this thesis strives to avoid. The methodological and scoping decisions made as a result of engaging with this literature are summarized in Table 3.1 at the end of subsection 3.2.4.

3.2.1 Methodological Instructions within the ACF

Several papers by Sabatier and his co-authors contain practical instructions for researchers wishing to apply the ACF in their work. Weible and Sabatier mention that applications of the framework typically involve questionnaire and interview data or an "analysis of documents and reports" (2006, p. 132). The most detailed guidance for applying the ACF can be found in the Methodological Appendix of Sabatier and Jenkins-Smith's 1993 book, where they detail how elite beliefs and policy positions can be studied using content analysis of public documents. However, some of these strategies can also be adapted for conducting and analyzing interviews. According to the authors, an ACF-based content analysis consists of (1) the identification of the sample within the target population to be coded, (2) the development of a coding frame based on the relevant elements of the target population's belief systems, and (3) measures to ensure validity in inferring beliefs from the sources. (1) The target population includes representatives of the policy subsystem who have attempted to influence policy developments. The reputational (or snowballing) sampling technique, whereby "identified elites" are "asked to list other elites," has been chosen for the interview-based portion of this thesis to ensure that the sample contains the most important actors of the policy subsystem (Jenkins-Smith & Sabatier, 1993, p. 241). (2) Pierce et al. (2022) recommend identifying at least two policy core beliefs per coalition, as well as evidence of coordination (which may include sharing information and other resources). According to Jenkins-Smith and Sabatier (1993), a coding frame based on the ACF is designed to capture the subject's position within the range of possible beliefs, which are also divided into the three levels (from deep core beliefs to secondary aspects). Variables pertaining to beliefs can be supplemented by other types of data corresponding with different components of the ACF. Coding frames typically go through several iterations, as their preliminary versions are often

refined after being applied to the material (Jenkins-Smith & Sabatier, 1993). The development of a coding frame using these instructions as a point of departure is described in the subsection 4.3.2; the coding frame itself is included in **Appendix D**. (3) Jenkins-Smith and Sabatier (1993) maintain that attention needs to be paid to issues of validity. Validity of the coded material is low when a speaker is not expressing their true opinion, which occurs when they "tailor their arguments to fit a specific audience" (Jenkins-Smith & Sabatier, 1993, p. 243). Following the authors' recommendations, three mitigation measures have been adopted in this thesis. Firstly, because the propensity to voice different beliefs in different contexts diminishes as the seniority level of the speaker increases (Jenkins-Smith & Sabatier, 1993), the most senior-level experts possible (rather than randomly sampled policy actors) were approached for interviews. Secondly, to garner their true opinions, unfiltered by self-moderation when discussing controversial topics, interviewees were assured that they would not be identified by name or professional title in this thesis. Thirdly, the open and semi-structured interview format allowed subjects to use their own frame of reference instead of, for example, one imposed by overly leading survey questions (where responses would be "artifacts of the instrument" (Shanahan et al., 2018, p. 339)), ensuring that their views be captured and represented accurately (Jenkins-Smith & Sabatier, 1993). This is also a reason why a qualitative data analysis approach was judged to be superior to a quantitative one in this thesis.

In his original paper presenting the ACF, Sabatier (1988) formulates an "official" list of 9 hypotheses, which encapsulate key principles of the framework; Sabatier and Weible's 2007 revision of the framework expands the list to 12 standard ACF hypotheses, which are thematically divided into those concerning advocacy coalitions, those related to policy change, and those on policy-oriented learning. (Pierce et al. (2022, p. 146) call these three terms "the main dependent variables" of the ACF). In addition, the authors pose multiple questions about the causal relationships between different aspects of the framework, which they invite researchers to explore and test in different empirical settings (Sabatier, 1988; Sabatier & Weible, 2007). Hence, in addition to applying the framework to model a specific policy subsystem or to explain the policy processes therein, papers drawing on the ACF could also explicitly validate ACF's core hypotheses. ACF applications can also help expand the "research program" (Sabatier, 1988, p. 159) and contribute to "long-standing debates within the ACF" (Sabatier & Weible, 2007, p. 197) such as those about the conditions fostering cross-coalition learning, those regarding coordination within coalitions, and those about subsystem interdependencies (Weible et al., 2009). While this is not the main motivation for this thesis, some of these questions and several ACF hypotheses are addressed in the discussion section.

3.2.2 Lessons from Past Applications of the ACF

Further, inspiration has been obtained from reviews on the trends in past applications of the ACF. Weible et al. (2009) analyze 80 applications of the ACF published globally between 1987 and 2006. Pierce et al. (2022) follow up on this work with their analysis of 161 ACF applications from 2007-2014. Nohrstedt and Olofson (2016) review 25 such applications in the context of Swedish policy spanning the years 1998-2015, while Jang et al. (2016) cover 67 applications of ACF in South Korea from 2002 through 2014. In their editorial of a journal special issue devoted to applications of the ACF, Weible et al. (2011) introduce a compilation of 8 articles. Drawing on a total of over 300 studies applying the ACF, these five review papers provide highly valuable insights – summarized in the following three paragraphs – on the most common research objectives, most frequently used data collection and analysis methods, and the pitfalls to avoid in applying the ACF.

First, past ACF applications' research objectives will be discussed to demonstrate that the formulation of the research question guiding this thesis was informed by common approaches from previous inquiries. ACF applications reviewed in the five papers cited in this subsection employ the framework in relation to a wide variety of policy domains, from national security to educational policy, which is a testimony to its versatility and thus also suitability to digital policy. As for the extent to which past ACF applications' main research objectives are borrowed from the framework itself, Weible and colleagues' (2009) stocktaking exercise reveals that only 45% of the reviewed papers explicitly test one of the ACF hypotheses; of these, most focus on the effect of external perturbations on policy change, the stability of coalitions, and on policy-oriented learning in a forum or in a situation defined by intermediate conflict. Pierce et al. (2022) highlight a selection of highly cited and methodologically sound ACF applications, which they divide into three categories based on their research objectives. The first category comprises studies of advocacy coalition membership and structure, which the authors consider "the most methodologically established part of the ACF" (Pierce et al., 2022, p. 146) especially thanks to the availability and wide usage of Jenkins-Smith and Sabatier's (1993) methodological appendix introduced above. (This is the category where this thesis would be placed.) The second category of ACF applications seeks to understand the degree of policy change over time and the third one is concerned with policy-oriented learning, which is typically studied by examining whether beliefs or strategies change in light of new information (Pierce et al., 2022). Similarly, Nohrstedt and Olofson (2016) find that 64% of the reviewed Swedish ACF applications focus on identifying coalitions and understanding their beliefs and policy positions; 64% of the applications also seek to explain policy change, mostly through coalition structure or learning. The most common research objective in the works reviewed by Jang et al. (2016) was to explain policy change, mainly due to external subsystem shocks (63% of the cases) or as a result of policy learning (34%); only 4.5% of these articles

formally tested any of the traditional ACF hypotheses. Lastly, the most commonly posed research question in the ACF applications discussed by Weible et al. (2011, p. 353) is "What is the structure of advocacy coalitions?" (in 50% of the articles, of which one additionally considers their stability and one their effect on policy change). Taken together, the review papers suggest that it is not uncommon to use the ACF as an aid in mapping the structure of a policy subsystem and its context (or, in Sabatier's words, "a useful ordering framework for identifying important variables and relationships" (1998, p. 120)), without formally testing any of the standard ACF hypotheses. This was deemed to be the best approach for the policy problem investigated in this thesis, as this is, to the author's knowledge, the first time European digital sovereignty in the context of government cloud computing has been analyzed through the lens of the ACF. Hence, an initial outline of the main coalitions' membership and their policy beliefs is judged to be a research objective of an appropriate scope.

Second, customary methods of data collection and analysis in past ACF applications will be outlined to justify the methodological choices made in this thesis. The most common data collection method in the articles reviewed by Weible et al. (2009) – after the 41% of articles that left the method unspecified – was interviews (20%). In addition, 10% of the articles combined interviews and content analysis, 10% combined questionnaires and interviews, and 9% used content analysis only. Articles published in the subsequent years seem to have a stronger methodology. Pierce et al. (2022), who do not disaggregate articles using one data collection method from those using two, report that 67% of the reviewed ACF applications used interviews, 60% used document analysis (based on sources including public documents, government documents, newspaper articles, or documents from policy actors), 60% used both, and 18% performed surveys. 91% of the articles used some form of qualitative analysis, while only 23% used quantitative data analysis (e.g., network or cluster analysis) (Pierce et al., 2022). In Nohrstedt and Olofson's (2016) findings, content analysis is the most frequently used data collection method (in 38% of papers), followed by papers with an unspecified methodology (28%) and those drawing on interviews (22%). The most popular data analysis methods were interpretive approaches and mixed methods (each used in 32% of cases), followed by qualitative (in 18% of the cases) and quantitative (7%) approaches (Nohrstedt & Olofsson, 2016). Surprisingly, Jang et al. (2016) report that as many as 85% of the reviewed applications of the ACF did not articulate their data collection approach, while 7.5% of the papers used interviews. Of the 8 articles discussed by Weible et al. (2011), 50% relied on questionnaire data and 37.5% used content or document analysis (in one case together with interviews). The vast predominance of ACF applications drawing on interviews, document/content analysis, or both led to the decision to base the methodological design of this thesis on a combination of these two data collection methods, coupled with qualitative data analysis. These choices are also congruent with Weible and Sabatier's recommendations mentioned above (2006).

Third, relevant recommendations based on past (mis)applications of the ACF will be highlighted, including those regarding the time perspective. Weible et al. (2009) point out some of the most frequently overlooked aspects of the ACF, which include policy brokers, the role of coordination within a coalition, and the relatively stable parameters that are external to a subsystem. Therefore, these aspects were also incorporated in the coding ACF-based frame used in this thesis to ensure their inclusion (see **Appendix D**). In addition to urging researchers to clearly specify their data collection and analysis methods (see above), Weible et al. also critique attempts to integrate stages of the policy cycle into the framework, as challenging such linear policymaking models is one of the ACF's very raisons d'être (2009). Weible et al. (2011) note that many ACF applications take a shorter perspective than the "decade or so" envisioned by Sabatier – some studies only consider one year or less. Similarly, Pierce et al. (2022) include both cross-sectional and longitudinal studies among their model ACF applications. In response, Weible et al. (2011) concede that the long time perspective is "more applicable to some research questions than to others" but advise that studies using a shorter duration "should be seen in the context of the longer-term dynamics of the subsystem" (p. 354). As the policy problem investigated in this thesis only has a history of a few years, a medium time perspective is adopted, but longer-term dynamics are considered.

3.2.3 The ACF in the Context of EU-Level Policymaking

The intended geographical scope of this study encompasses both EU-level policymaking and national-level political processes that give rise to Member States' positions. Therefore, the relationship between the different levels from the perspective of the ACF needs to be clarified. While the ACF was not specifically developed with the supranational scope in mind, the creator of the framework considers it almost universally applicable, especially after the 2007 revision. In fact, Sabatier (1998) argues that the ACF offers multiple advantages for studying EU policy processes: the ACF's recognition that policy subsystems are dynamic and often nested within each other fits well with the EU's multilevel governance system; the framework's distinction between core and secondary aspects of policy can help classify different policy initiatives at different administrative levels; and coalitions' "venue-shopping" described within the ACF "certainly seems to be happening" in the EU, "both among levels of government and among institutions at the European level" (p. 121).

Several authors use the ACF to challenge intergovernmentalist theories and the assumption that the EU "depoliticizes political issues" (Beyers & Kerremans, 2004, p. 1119). Radaelli (1999), who focuses on EU-level advocacy coalitions concerned with direct tax policy, contrasts the relative fluidity of the political architecture and processes of the EU with the more rigid political processes of its Member States. Building on Smyrl (1998), Radaelli's

(1999) most interesting contribution is his argument that the European Commission is not always best conceptualized as an agent of Member States and a forum for intergovernmental deliberation, but rather a "self-motivated, autonomous" policy actor (Smyrl, 1998, p. 82). Radaelli describes how the Commission succeeded in breaking the boundaries between two opposing coalitions by "exploiting the loose characteristics of EU public policy-making" and portraying itself as a neutral policy broker, but in reality acting as an advocacy coalition member in its own right and shaping the beliefs of Member States by "providing conceptual innovation and by engaging in reasoned persuasion" (1999, p. 665). Similarly, Brooks discusses the contrasting pharmaceutical policy positions held by different policy participants within the Commission, resulting in different Directorates-General being members of opposing advocacy coalitions (2018). That is why members of three different Directorates-General are interviewed in this thesis.

Various studies applying the ACF in the context of EU policymaking were reviewed to understand how scholars conceptualize the relationship between policy subsystems at different levels of administration, as many of the policy actors portrayed in this thesis participate in, for example, both national-level and EU-level policymaking. Yilmaz (2018) focuses on a single advocacy coalition within the EU sports policy subsystem, but he divides the actors within the coalition into two subgroups – "EU policy actors," i.e., those interacting with EU institutions, and "the stakeholders," pan-European organizations representing sports associations and leagues who are active in the advocacy coalition but typically do not engage with the EU directly (pp. 357-359). Van Eerd and Wiering's (2022) application of the ACF revolves around Member States, which are shown to form a "traditional" North-South dichotomy in the question of EU water governance. They also usefully link the ACF to the EU "policy process spiral," where powerful Member State advocacy coalitions, with strong domestic networks as a basis, shape the process whereby policies are continuously "uploaded, downloaded, and reloaded" between domestic and the EU level (van Eerd & Wiering, 2022, p. 580). Beyers and Kerremans describe sector-specific networks around Commission bureaucrats and observe that domestic political cleavages are transferred into the political space of the EU, where they are mobilized by advocacy coalitions (2004). Büttner et al. (2015) highlight the role of "EU Affairs professionals," a stratum of experts between EU, national, and regional levels of policymaking, who may either act as interlocutors between the different levels (and contribute to the formation of policy networks and advocacy coalitions), or reinforce the disconnection between them. Koch and Burlyuk (2019) situate EU policymaking in a global context, unpacking the structure of two transatlantic advocacy coalitions around EU conflict minerals legislation, and analyzing the role of other intergovernmental organizations such as the OECD and the UN. This brief review of the most pertinent literature shows that scholars either do not treat policy subsystems at different administrative levels as separate units, or view EU-level coalitions as an extension of national-level ones.

3.2.4 Summary of Methodological and Scoping Decisions

→ This subsection discussed a selection of articles that described how to apply the ACF, reviewed previous ACF applications, or directly applied the framework in the context of EU-level policymaking. This was done to ensure that the framework be applied correctly in this thesis – that is, in ways that do not radically depart from the intentions of those who created the ACF and from common practices in the extensive body of ACF applications. In the process of reviewing this literature, several decisions related to the scope and methodology of this thesis were made, which are summarized in Table 3.1 below. Additional aspects of the decisions related to data collection and analysis, made for reasons unrelated to the "demands" of the theoretical framework, are described in detail in subsection 4.2 (research design).

Category	Decision	ACF-related justification
Research objective	Describe the structure of the nascent advocacy coalitions around the eGovernment cloud debate; ACF's formal hypotheses not to be tested	The majority of ACF applications describe coalition structure without formally testing an ACF hypothesis (Pierce et al., 2022; Weible et al., 2009)
Data collection method	Open or semi-structured interviews with 10+ experts familiar with the policy subsystem & content analysis of documents provided by the interviewees (see also subsection 4.3.1)	Interviews and content analysis are the most common data collection methods among ACF applications (Nohrstedt & Olofsson, 2016; Pierce et al., 2022; Weible et al., 2009). Policy elites are chosen (but not personally identified in the thesis) and asked open-ended questions to maximize validity (Jenkins-Smith & Sabatier, 1993).
Data analysis method	Qualitative, based on a combination of open coding and an ACF-based coding frame (see also subsection 4.3.2)	This decision follows select instructions from Jenkins-Smith and Sabatier's (1993) methodological appendix and is in line with established practices (Nohrstedt & Olofsson, 2016; Pierce et al., 2022)
Time perspective	Medium-term – approximately 3 years; longer-term dynamics are addressed; cross-sectional in nature (see also subsection 4.2.5)	While Sabatier (1988) originally intended the ACF solely for studies with a long time perspective, scholars have successfully applied it to short and medium time perspective studies as well (Pierce et al., 2022; Weible et al., 2011)
Geographical scope	Both EU and national levels (EU-level coordination, with special attention to the role of the European Commission and two Member States representing the opposing coalitions)	Past work, esp. Radaelli (1999), van Eerd & Wiering (2022), and Beyers & Kerremans (2004), demonstrated the applicability of the ACF to national and EU level policy processes at the same time

Table 3.1 Summary of methodological decisions made after engaging with the ACF literature

4 Methodology

This methodological chapter is divided into four sections. The first section outlines the literature search methodology that underpins chapters 2 and 3, the second section details the decisions made when designing the research, and the third one is dedicated to the research methods (i.e., data collection and analysis) used in this thesis and the considerations related to the quality of the research inquiry. The fourth section discusses the standards of ethical conduct reflected in the methodological choices made in this study.

4.1 Literature Search Methodology

A literature search was undertaken to define and contextualize the main terms of the research question and to understand how to apply the conceptual framework in this thesis. The results of this search are presented in chapters 2 (literature review) and 3 (conceptual framework). This section discusses the methodological choices behind the literature search, which are intended to establish congruence between the research question and the literature review strategy (Morse et al., 2002, pp. 17–18) and to maximize the rigor of the subsequent research (Templier & Paré, 2015).

A combination of four frameworks informs the design and structure of the literature search. They originated, respectively, in the fields of business, education and psychology, software engineering, and information systems, but have been applied across domain boundaries. (1) Snyder (2019) breaks the process of conducting a literature review down into four phases – designing the review, conducting the review, analysis, and writing up the review (pp. 336-337) –, where her guidelines for the first phase are especially instructive. In order to design the review appropriately, (a) the purpose of the review needs to be clearly established; (b) the type of literature review has to be selected; (c) the intended audience of the review should be considered; (d) a preliminary literature search may be conducted in order to identify literature reviews that already exist; and (e) a search strategy must be developed (Snyder, 2019, pp. 334–337). (2) Another framework that has been used to inform the procedures underlying the work presented in this section Is Cooper's taxonomy of literature reviews, which draws authors' attention to six main characteristics of literature reviews: (a) focus (regarding the type of material that is of central interest to the reviewer); (b) the goal of the review; (c) perspective; (d) exhaustiveness of coverage; (e) organization of the review; and (f) the intended audience (1988, pp. 107–112). (3) Kitchenham and Charters (2007) outline three relevant activities defining the planning stage of a (systematic) review: (a) identification of the need for a review (in relation to existing reviews on the same topic); (b) specifying the research question(s) (which may be subject to revision throughout the planning phase); and (c) developing a review protocol (pp. 6–13). Finally, (4) Templier and Paré call the first step of the procedure for conducting literature reviews

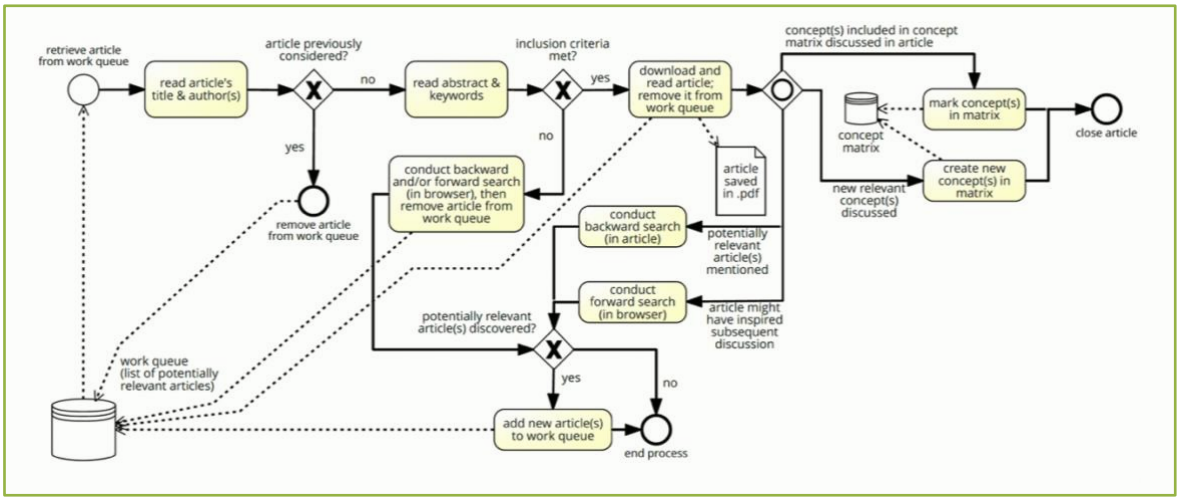
Category	Choice made	Justification
- Preliminary literature review *(1)(d)*; - Need for a review *(3)(a)*	- A preliminary literature scan, based on a series of keyword searches, was conducted. Based on 32 retrieved sources (of which 21 were academic papers and 11 policy documents), the first version of the research question guiding this thesis was formulated, and a methodology for a systematic literature review was outlined. One of the first clear observations following the literature scan was that there is a lack of agreement on the meanings of several central terms. - A separate query was performed in search for recent review articles covering the terms "digital sovereignty" and/or "data sovereignty," and (only) one was found, namely Hummel et al. (2021). While its coverage is exceptionally comprehensive (Hummel et al. (2021) reviewed 341 papers), it was decided that the literature review conducted as part of this thesis will not constitute a duplicate effort to this paper.	- Reasons why it was judged worthwhile to perform a literature review covering similar themes as Hummel et al. (2021) include: (i) the literature considered in the review had a cutoff in November 2019, calling for a follow-up review covering the past 3 years of developments; (ii) aiming to map the various ways in which different notions of digital sovereignty are understood in academic journals, the focus of the above review is very broad (enumerating the different possible notions, agents, contexts, and values involved), whereas the present literature review aims to provide more detail on the relevant substantive discussions on digital/data sovereignty.
- Purpose of the review *(1)(a);* - Goal(s) of the review *(2)(b), (4)(a)*; - Research question(s) addressed *(3)(b)*	- The goal is (i) the identification of central issues and, given the lack of conceptual clarity mentioned above, (ii) a generalization formulated from multiple specific instances (Cooper, 1988). Specifically, this translates to the following aims: (I) to define and contextualize key terms and concepts related to "European digital sovereignty" (chapter 2); (II) to define and contextualize key terms and concepts related to "government cloud computing" (chapter 2); and (III) to review material that can aid in understanding and correctly applying the conceptual framework (the advocacy coalition framework) (chapter 3).	- Rather than being a standalone publication, this literature review constitutes just one part of a graduate thesis. Therefore, its purpose is not to directly answer the research question stated in the *Introduction* section. Instead, the three aims motivating the work presented in this chapter are a necessary partial step towards building a sound methodology addressing the research question. - The literature review is also conducted with the aim of uncovering a gap in the extant research for this thesis to fill.
- Focus *(2)(a)*; - Boundaries of the review *(4)(c)*	- The focus of *aims (I)* and *(II)* was be definitions and research outcomes; *aim (III)* was primarily concerned with research theories, followed by research outcomes	- Selected papers were read in their entirety but keeping the *focus* in mind helped structure (and expedite) the review process.
- Type of review *(1)(b)*; - Coverage *(2)(d)*;	- A systematic review was deemed most suitable. - Its coverage is exhaustive with selective citation (Cooper, 1988).	- The preliminary literature scan revealed that the relevant body of literature has a relatively short history, rendering exhaustive coverage feasible.
- Perspective *(2)(c)*	- A neutral perspective is espoused while presenting the facts and arguments found in the reviewed literature.	- The literature was reviewed to objectively characterize the literature landscape rather than to prove a particular point of view.
- Organization *(2)(e)*; - Concepts at the heart of the review *(4)(b)*	- The literature review is arranged conceptually. The literature is presented in the order dictated by the sequence of the topics covered in chapter 2	- The alternatives, i.e., chronological organization or an author-centric approach (Webster & Watson, 2002), would not be suitable for an emerging field.
- Intended audience *(1)(c), (2)(f)*	- The intended audience consists primarily of students and academics in the fields of e-government, public administration, and information systems.	- The subject of this thesis is associated with these disciplines. The literature informing this study is mostly a product of these fields, too.

Table 4.1 Literature search design choices and their justifications

"formulating the problem," which consists of (a) specifying the review's primary goal(s), (b) clearly defining the concepts at the heart of the review, and (c) establishing the review's boundaries (2015, pp. 115–116; 124–125). Table 4.1 above summarizes the literature review design choices made in the planning phase, along with their justifications based on the four frameworks outlined above. Each category is associated with a number and letter based on the above overview (e.g., "*(2)(a)*" represents the first characteristic of Cooper's taxonomy – focus), or more than one letter-number combination, highlighting conceptual overlaps among the frameworks used.

Importantly, several authors note the iterative nature of the review process, with many decisions made in the planning stage often being subject to refinement in later stages in light of new information (Kitchenham & Charters, 2007; Templier & Paré, 2015). Instances of such versioning are disclosed in **Appendix I**, where the evolution of the research question is discussed.

The literature search was conducted in three parts, as each of the three aims (see Table 4.1) called for slightly different search and inclusion parameters. Nevertheless, a consistent search strategy was followed: (1) Each aim was converted into a set of keywords, which formed the initial search string (the OR operator was used to include multiple similar search terms in one string rather than performing multiple separate searches). (2) The initial search string was used to query the titles, abstracts, and author keywords in two widely used online citation databases – Web of Science (WoS) and Scopus, (in this order) – and (in the case of aims (I) and (II)) one EndNote package curated for Digital Government research, namely version 17.5 of the Digital Government Reference Library (DGRL), which has been shown to include relevant peer-reviewed articles not captured by WoS and Scopus (Scholl, 2021; Zuiderwijk et al., 2021). Two filters were applied: one was language (only English articles were considered) and the other was related to the document type – only peer-reviewed journal articles, peer-reviewed conference papers, and book chapters were considered (for the sake of brevity, this section refers to all these document types as "articles"). No restrictions were imposed with regards to the timeframe, subject area, citation count, etc. – the sole exclusion criterion applied to the articles returned by each search, was the lack of availability of the full text document. After the exclusion of such results, all remaining records were placed in a "work queue" – a list of potentially relevant articles. The number of work queue items yielded by each database for each search string can be found in **Appendix J**. (3) Next, each individual article from the work queue was approached in a uniform manner, as modeled in Figure 4.1 below.



Source: author's own work

Figure 4.1 A BPMN model depicting the uniform process of selecting articles for inclusion in the literature review

After removing duplicate articles, the title, author keywords, and abstract of each article were read in order to evaluate whether the article meets at least one of the inclusion criteria formulated for each search string (please refer to **Appendix J**). Crucially, the majority of articles identified through the keyword search (including those that missed the inclusion criteria) was subjected to a backward and forward search for further relevant sources (Webster & Watson, 2002).

4.2 Research Design

Research design is the general strategy of how the research question will be answered. Some elements of this strategy are outlined in chapter 1; this section lays out further details, following the sequence of choices suggested by Saunders et al. (2012), who argue that decisions regarding data collection and analysis (to which they refer as "techniques and procedures") should be preceded by decisions about five "underlying issues" (pp. 126-128). These five issues – namely the research philosophy, the research approach, the methodological choice, the research strategy, and the time horizon – are addressed in the following five subsections and ultimately summarized in Figure 4.2, an adaptation of Saunders and colleagues' "research onion" (2012, p. 128), at the end of this section.

4.2.1 Research Philosophy

Research philosophy refers to the way in which a researcher views the world, which shapes the assumptions about the nature of the knowledge produced in his or her research project (Saunders et al., 2012). Social science reporting conventions require that researchers reflect on and explicitly articulate their otherwise taken-for-granted epistemological and theoretical

presuppositions, in order to demonstrate that the logic of their inquiry is sound (Ospina et al., 2018). The outer layer of the "research onion" is a repertoire of four research philosophies[34] to choose from – pragmatism, positivism, realism, and interpretivism (Saunders et al., 2012). Most likely inspired by the work of Larry Laudan and other philosophers of science, Saunders et al. place these philosophies on a "multidimensional set of continua" along three main axes: ontology (the nature of reality or being), epistemology (what is considered acceptable knowledge), and axiology (the role of values in research) (2012, pp. 129; 140). Hence, a reflection on one's research philosophy based on Saunders et al. (2012) should address all three dimensions.

The research philosophy underpinning this thesis is interpretivism – the most common approach in public administration research (van Thiel, 2014). The interpretivist school of thought is associated with a subjectivist ontology, which understands reality, identities, and knowledge as socially constructed phenomena, which are in a constant state of revision through social interactions (Patterson & Williams, 1998; Saunders et al., 2012). Research investigating these social constructs assumes that humans behave "as if their constructed reality" were "the actual reality," which makes the positivist notion of an objective, measurable reality irrelevant (Halkias et al., 2022, p. 5). Interpretivist epistemology emphasizes the uniqueness of social phenomena and knowledge produced by social actors, which cannot be fully grasped through techniques originating in the (fundamentally distinct) realm of the natural sciences (Bryman, 2012; Saunders et al., 2012). Knowledge is seen as contextual and time-bound; understandings are subject to revision (Patterson & Williams, 1998). Interpretivism is more concerned with understanding human behavior (and the subjective meanings around it) than it is with explaining or predicting it by analyzing the "forces that are deemed to act on it" (Bryman, 2012, p. 28). Interpretivist axiology acknowledges that research is value bound and that the researcher is part of the research process, yet committed to understanding and accurately representing research subjects' point of view (Bryman, 2012; Patterson & Williams, 1998; Saunders et al., 2012). In interpretivist research, values are made explicit (Walliman, 2011); in this thesis, this is reflected, for example, in section 4.3.3, where the researcher's subjectivity is acknowledged and reflected upon with respect to the potential biases it might produce (see). The interpretivist research philosophy is fully compatible with the ACF, the conceptual framework chosen for this thesis, which assumes that individuals interpret the world through

[34] This list of four research philosophies, which is intended for business and management researchers, roughly corresponds with what some other disciplines (such as Information Systems) call research traditions or "research paradigms" (Gregor, 2006). However, in Saunders et al. (2012), "research paradigms" refer to something else, namely ways of examining social phenomena through the lens of two conceptual dimensions: subjectivism versus objectivism, and a radical (i.e., motivated by social change) versus regulatory (i.e., not socially critical) view of organizational affairs (pp. 140-143). These dimensions produce a matrix of four research paradigms, which are however not included in the 2012 version of the "research onion" and therefore not discussed in this thesis.

the lens of their subjective (core and policy-oriented) beliefs and construct meaning through social interactions within their political environments. This meaning motivates the formation of action-oriented groups, often holding opposing views on a policy issue – neither of which is presumed by the researcher to be closer to an "objective truth." While the ACF's causal mechanism, together with its associated set of testable hypotheses, lends itself well to studies that are positivist in nature, this thesis is not one of them, as its aim is simply to use the framework as an aid in modeling the coalition structure. The following subsections demonstrate that the research design of this work is consistent with interpretivism.

4.2.2 Research Approach

Research approach describes the role of theory (i.e., a system of ideas intended to explain the relationship between key variables) in a research project. According to Saunders et al. (2012), there are three main research approaches, corresponding with three basic forms of reasoning: deduction, induction, and abduction. Deductive reasoning starts with a theory and investigates a case to either verify or falsify the rule (Timmermans & Tavory, 2012). Inductive reasoning does the opposite – it begins with a case (or a collection of cases) and explores it in order to identify themes and patterns, to infer that some universal rule is operative, and to generate a new theory (Saunders et al., 2012; Timmermans & Tavory, 2012).

This thesis applies the abductive approach, which combines elements of both deduction and induction as it moves back and forth between the specific and the general (Saunders et al., 2012). Abduction seeks a "situational fit between observed facts and rules," starting with the consequences (usually, a surprising fact) and then constructing the reasons (Timmermans & Tavory, 2012, p. 171). In other words, it is a process of "developing guesses" – of choosing, suggesting, or constructing an exploratory hypothesis, which is thereafter evaluated (Potschka, 2018, p. 24). In line with the interpretivist philosophy, abduction grounds a theoretical understanding of the studied context in the worldviews and perspectives of the research participants; it then proceeds to develop a social scientific account of these perspectives (Bryman, 2012). This accurately describes the highly iterative research process of this thesis, where the initial round of data collection informed the selection of the theoretical framework, which was then tested through a subsequent round of data collection and analysis, from which yet further theoretical observations emerged (Saunders et al., 2012). The abductive element of this thesis is the empirically-based proposition that EU Member States can be divided into three coalitions based on their motivations and position in the European digital sovereignty debate (rather than two, as claimed by Baischew et al. (2020)).

4.2.3 Methodological Choice

The methodological choice starts with considering the fundamental distinction between qualitative and quantitative research. At the core of this distinction is the kind of data with which each research type is concerned – words in the case of qualitative research and numbers in the case of quantitative research (Bryman, 2012). Qualitative research design usually goes hand in hand with an interpretive philosophy and induction or abduction, as the studied phenomena usually entail subjective and socially constructed meanings, which the researcher works to access and understand (Saunders et al., 2012). Quantitative research design is generally associated with positivism and the highly structured data collection and analysis techniques of the deductive approach (Saunders et al., 2012). In addition, Saunders et al. (2012) distinguish between "mono method" studies, which use a single data collection technique, and "multiple method" studies, which use more than one (pp. 164-166). The latter are further divided into "multimethod" studies, which draw on more than one data collection technique within either the qualitative or the quantitative domain, and "mixed method" studies, which combine both qualitative and quantitative research (Saunders et al., 2012, pp. 164–166).

Following the research question and objectives, this thesis deals solely with non-numerical data. It is based on a combination of two data collection techniques – interviews and document analysis. Therefore, it can be described as a multimethod qualitative study.

4.2.4 Research Strategy

The creators of the "research onion" list a relatively wide palette of possible research strategies – experiment, survey, archival research, case study, ethnography, action research, grounded theory, and narrative inquiry – while admitting that these genres can be somewhat blurred in practice (Saunders et al., 2012). The choice of a research strategy is guided by the requirements of the research question and objectives, but also by pragmatic concerns such as the amount of time and other resources at the researcher's disposal, as well as access to potential participants and other sources of data (Saunders et al., 2012; van Thiel, 2014). The author of this thesis admits that the access to certain interviewees (especially those associated with the European Commission) and the availability of certain documents, played a significant role in the decision to focus on these settings over others and to use a both interviews and document analysis as a data collection technique. These considerations affected the choice of the research strategy.

This thesis is a case study – the predominant research strategy in the field of public administration (Ospina et al., 2018). A case study is an in-depth, holistic examination of a specific phenomenon within its real-life context, with the aim of rendering detailed

and extensive descriptions (Saunders et al., 2012; van Thiel, 2014). Building on the work of Robert Yin, Halkias et al. suggest that case study design is deemed to be an appropriate research strategy if three conditions are satisfied: (1) if the research question is explanatory ("how?" or "why?") or descriptive ("what?"); (2) if the focus of the study is on contemporary events; and (3) if the researcher cannot control behavioral events (2022). This thesis fulfills all three conditions – the research question is a descriptive one; European digital sovereignty is a subject of high contemporary relevance; and the researched context is not one where the researcher could experimentally manipulate behavioral events. A case "can be almost anything" – a group of people, an organization, a city, and event, a project, a process, a law, a decision, etc. (van Thiel, 2014, p. 86). However, it is useful to clarify the research domain which the case represents and to draw a clear line between the case itself and the unit of study (Bryman, 2012; van Thiel, 2014). In this thesis, the case under investigation is the policy problem of European digital sovereignty in government cloud computing. The general domain to which this case belongs is policy (one at the intersection of several policy domains, such as digital technology, government innovation, cybersecurity, but also industrial policy). The sub-units studied within this case are clarified in the following paragraph.

Following Robert Yin, Saunders et al. (2012) make a distinction between four possible case study strategies, as each case study can be classified across two discrete dimensions. The first dimension concerns the number of cases, i.e., whether it is a single or a multiple case study. A *single case study* is reasonable when the results can be argued to have high external validity because the research subject is (a) extreme, unique (such as a recently passed law), critical, or revelatory (i.e., related to a phenomenon that has never been observed before), (b) (on the contrary) representative or typical (i.e., exemplifying a broader category of cases), or (c) especially suitable for a longitudinal study (Bryman, 2012; van Thiel, 2014). A *multiple case study* is advantageous if the author wishes to produce results that have broader applicability and generalizability, and thus potentially more impact, as a result of covering a range of contexts (Halkias et al., 2022). Typically, either homogeneous cases are selected because they are predicted to produce similar results, or heterogenous cases are chosen because the researcher expects the differentiating factor to lead to a variance in results (Saunders et al., 2012; van Thiel, 2014). This thesis is a single case study of a unique policy problem. The second dimension along which case studies can be divided refers to the unit of analysis – in this view, case studies can be either holistic, or embedded. In a *holistic case study*, the case (for example, an organization) is studied as a whole. In an *embedded case study*, the researcher chooses to focus on a number of sub-units within the case (for example, several organizational departments). (Saunders et al., 2012) This thesis can be considered an embedded case study that zooms in on the role of three sub-units participating in the discussions about the policy problem, namely the government of

France, the government of the Czech Republic, and the European Commission. The purposive selection of these sub-units (van Thiel, 2014) is addressed in subsection 4.3.1. It must be emphasized that these sub-units are deliberately not treated as multiple organizational or national cases to be compared against each other. This is because in the context of the European digital sovereignty debate, focusing on the relationships and interactions between the sub-units brings the analysis closer to the core of the issue than would a research design treating each case in isolation. A single, embedded case study research strategy was thus expected to yield the most insight on the subject.

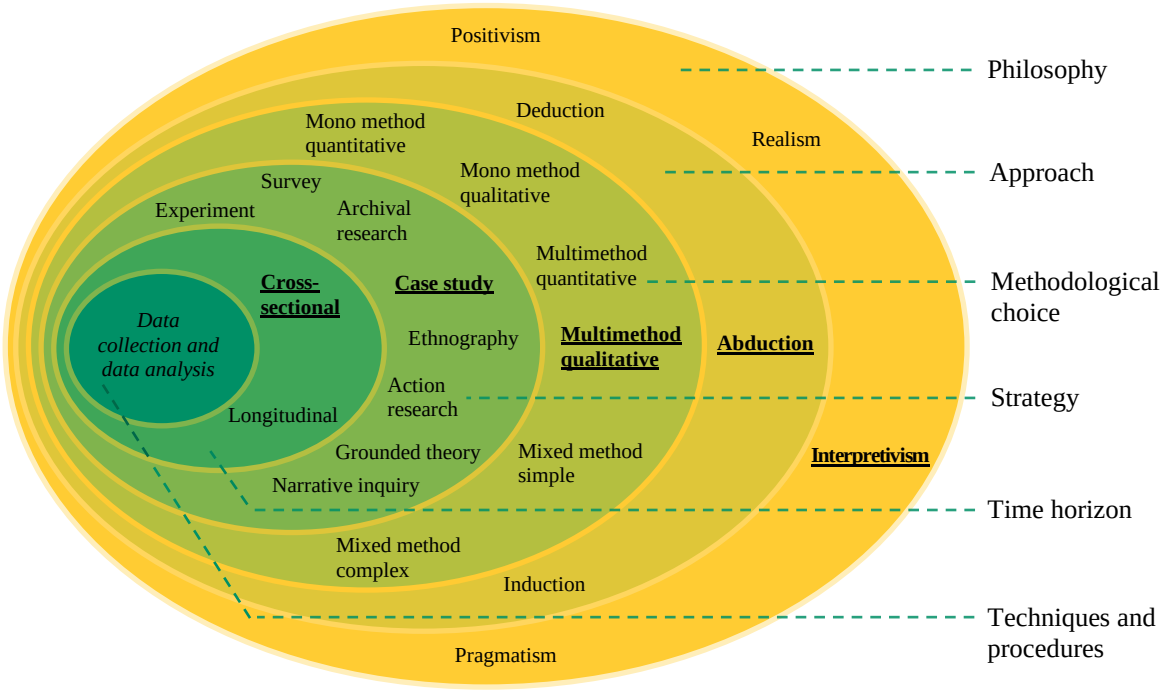
4.2.5 Time Horizon

The time horizon of a study refers to the length of the period that is covered. There are two basic types of studies: cross-sectional and longitudinal. A cross-sectional study is a "snapshot" of a phenomenon at a particular point in time, whereas longitudinal research investigates a subject as it develops and undergoes change over the course of time (Saunders et al., 2012).

This thesis is most accurately characterized as a cross-sectional study. The bulk of the primary data used in this thesis was collected via expert interviews conducted over the span of one month. Because some of these data points are reflections referring to past developments, the time perspective of chapter 5 encompasses approximately 3 years (as mentioned in **Table** 3.1). Nevertheless, the research design is not, for example, geared towards recording all relevant policy milestones or tracing their consequences over time; therefore, the time horizon is cross-sectional.

4.2.6 The Research Onion: Summary of Research Design Choices

→ The research design of this thesis is summarized in Figure 4.2, an adaptation of the "research onion" by Saunders et al. (2012). The five outermost layers of the onion correspond with subsections 4.2.1–4.2.5. Each layer is populated with a set of possible options proposed by Saunders et al. (2012), with the option chosen in this thesis marked in bold and underlined. The description of the core of the onion – data collection and data analysis – is written in italics, as it is not "covered" in the diagram. The techniques and procedures chosen in this thesis are discussed in the following section.



Source: adapted from Saunders et al. (2012), p. 128

Figure 4.2 The research design choices made in this thesis (underlined), depicted in the context of the other possible options within the "research onion"

4.3 Research Methods

Building on the research design, this section elaborates on the methods used in this thesis. First, the techniques and procedures used in the data collection and analysis stages are described. Next, measures taken to establish the quality of the research inquiry are outlined. The fourth subsection details the ethical considerations governing the choices made in this thesis.

4.3.1 Data Collection

Drawing on more than one data source type in a case study tends to yield better results than relying on a single type (van Thiel, 2014). Therefore, this study uses two methods of data collection – research interviews and document analysis – and the resulting data are then triangulated. Triangulation refers to the use of two or more independent data collection methods in order to cross-check the results wherever possible, thereby increasing the likelihood that the sources used are interpreted and understood accurately (Campbell et al., 2020; Saunders et al., 2012). In this thesis, this technique was used to ensure that the findings from document analysis corroborate the findings from interviews – a data collection method marked by several common sources of error, including misunderstanding

and memory problems on the part of the interviewee, as well as recoding and processing errors on the part of the interviewer (Bryman, 2012). Applying triangulation thus enhances the reliability and validity of the data (van Thiel, 2014).

The research interview – a conversation aimed at gathering valid and reliable information relevant to the research question (Saunders et al., 2012) – is an exceedingly common data collection method in case studies (Bryman, 2012). The purpose of the research interview is to gain a deep understanding of an individual's opinions, beliefs, experiences, or motivations with respect to specific matters (Gill et al., 2008). Interviews are particularly appropriate when exploring sensitive topics (where publicly available documents or group-based data collection methods would produce less genuine results), when the desired information cannot be obtained from alternative sources such as reports (e.g., due to its nonfactual or "unofficial" nature), and when detailed insights and reflections are required from respondents (Gill et al., 2008; van Thiel, 2014). All these conditions apply to the subject of this thesis, as explicitly confirmed by several interview participants.

There are three fundamental types of research interviews: fully structured interviews, semi-structured interviews, and open (also called unstructured or in-depth) interviews (Gill et al., 2008; Saunders et al., 2012). Structured interviews follow a predetermined, standardized list of questions posed to each respondent, in order to generate quantifiable data (Saunders et al., 2012). Semi-structured interviews are guided by an interview manual – a list of areas to be explored and possibly several specific prompts and key questions to be covered (van Thiel, 2014). However, which themes will be raised in a particular interview, and in which order, varies depending on factors such as the interviewee's perspective, experience, or preferences. In addition, the conversation may diverge from the preliminary outline to allow the respondent to elaborate on a key point or to pursue a relevant subject that may not have previously occurred to the researcher. (Gill et al., 2008; Saunders et al., 2012) The open interview is a less formal format where the informant is given the opportunity to talk freely about a specific topic – the initial question is the only fixed item across the different interviews (van Thiel, 2014). The aim is for the conversation not to reflect any preconceived theories on the part of the interviewer, letting the respondent's thinking process define the conduct of the interview (Gill et al., 2008; Saunders et al., 2012).

This thesis draws on 13 interviews conducted in July-November 2022, of which three are open and ten are semi-structured interviews. The open format was used at an early stage of the research process, where interviews can aid in refining the research question and objectives (Saunders et al., 2012). Once the research question was finalized and the conceptual framework was selected, largely based on the information gathered from the open interviews, an interview manual was created for the remainder of the interviews (see below). An anonymized list of interview participants, their respective organizations, and the interview types can be found in **Appendix A**. Of the 13 interviews, one took place in person,

10 were conducted via videoconferencing software, one took the form of a telephone call, and one was a written interview at the request of the interviewee (according to whom responses provided in writing were more thought-out and better worded than verbal answers). The duration of these conversations ranged from 45 to 90 minutes; the median duration was around 60 minutes. Of the 12 verbal interviews, nine were recorded and subsequently fully transcribed, while in three cases, the interviewer took simultaneous notes during the interview, from which interview reports were drawn up (van Thiel, 2014) (in one case, the intentional absence of a recording device best facilitated the informal atmosphere of a face-to-face exploratory conversation; in another case, a technical issue precluded the possibility of making a recording; and in one case, the respondent did not agree to be recorded). 10 of the conversations were in English, while three took place in Czech; however, the transcripts were translated into English for better comparability of results across all interviews in the coding stage.

The semi-structured interviews followed an interview manual (see **Appendix B**). An interview manual contains the following fixed elements: (1) an introduction, (2) the actual questions, and (3) a concluding section (van Thiel, 2014). (1) In the introductory part of the interview, the researcher reminded each participant of the context in which the interview was being conducted, the aims of the study, and the fact that the respondent would not be identified by their name or exact professional title in the thesis to increase the likelihood of honesty and minimize the effects of social desirability bias (Bryman, 2012; Gill et al., 2008). (This information had also already been communicated in advance via email.) Afterwards, the respondent was asked to give explicit permission for the conversation to be recorded and was assured that the recording was going to be deleted after being manually transcribed. The interviewee was also encouraged to answer questions both in a way that reflects the official position of the organization they represent, and in their personal capacity, in cases where these two perspectives might differ. (2) Being part of a study following an abductive research approach, the interviews were guided by a mix of questions derived from the conceptual framework and questions built around the "sensitizing concepts" following from the research objectives (van Thiel, 2014, p. 94). Care was taken to develop questions that are open-ended, neutral, sensitive, and unambiguous (Gill et al., 2008), but the interviewer also sometimes asked the participants to confirm or challenge her assumptions. Each interview started with personal factual questions and factual questions about others, but – in a reflection of a core component of the conceptual framework – also contained several questions about attitudes and beliefs (Bryman, 2012). In order to understand and interpret the respondents' perspectives as well as possible, effort was put in developing rapport with the interviewees, listening attentively, and posing frequent follow-up questions to probe deeper into some of their statements, for example whenever it was suspected that the interviewer and the interviewee might not share the same meanings of a term (Bryman, 2012; Corbin & Strauss, 2008; Gill et al., 2008). (3) In the concluding section, respondents

were asked to raise any points that have not come up during the interview but might be of interest to the researcher (and they were thanked for their valuable contributions). None of the interviewees expressed interest in validating the transcript.

The selection of interview respondents in this thesis can be described as purposive sampling – choosing participants in a strategic way, so that those interviewed are in an especially good position to provide insight into the research problem (Bryman, 2012; Morse et al., 2002). Because statistical inference is not part of the research design of this qualitative study, purposive sampling was deemed more suitable than probability sampling, where a random sample of policy actors would have been selected (Walliman, 2011) – which would, in this case, inevitably have consisted of individuals playing a less active role in shaping the European digital sovereignty debate than the actors selected in a purposive manner. As discussed in section 3.2.1, the ACF associates using policy elites as main data sources with higher validity than other types of policy participants. Therefore, most (but not all) of the interviews conducted can be described as elite interviews (van Thiel, 2014). In addition, as indicated in **Appendix A**, snowball sampling proved to be a useful technique (Bryman, 2012) – one interviewee often recommended another one as a great source of additional information on a given subject or as a particularly good representative of a certain perspective or opinion.

One form of purposive sampling is theoretical sampling (Bryman, 2012). Theoretical (or adaptive) sampling (Leung, 2015) – defined as "sampling on the basis of concepts derived from data" (Corbin & Strauss, 2008, p. 3) – is most closely associated with grounded theory, but it has been used in a range of inductive and abductive studies. According to Charmaz (2006), the purpose of theoretical sampling is to elaborate and refine the theoretical categories that begin to emerge in the process of analyzing data; as sampling is conducted, the researcher develops the properties of these categories until categories are saturated with data – that is, until no important new properties emerge anymore. Thus, data collection and data analysis are not two distinct stages – rather, the processes of data gathering and data analysis are concurrent, and interim results inform further data sampling decisions based on the informational requirements of the research project (Bryman, 2012; Charmaz, 2006; Morse et al., 2002). Although this thesis had no ambition of developing a standalone, novel theory, theoretical sampling is a fitting label for the process of making sampling decisions as theoretical insights emerged while data coding was in progress. Most notably, the understanding that different Member States, but also different national-level organizations, can be broadly grouped into two categories depending on their stance on specific issues within the digital sovereignty debate, only emerged halfway through the data collection and analysis process, leading to the decision to motivate subsequent interviews by testing if the ACF – or a slightly modified version thereof – might be a fitting theoretical lens through which to

understand the research problem. Both further selection of participants and the categories used in the coding scheme were adjusted accordingly at that stage.

As discussed above, this is an embedded case study; therefore, it is prudent to not only explicitly justify the selection of the interview participants, but also clarify the sampling strategy of the case sub-units to which the interviewees belong (Ospina et al., 2018). The sampling process can thus be divided into two levels: *sampling of context*, corresponding with the sub-units, and *sampling of participants* within each context (or case sub-unit) (Bryman, 2012). As clearly identified in **Appendix A**, there are three main case sub-units on which this thesis focuses: the French government, the Czech government, and the European Commission. As is explained in detail in chapter 5, these sub-units represent two opposing views on key questions within the digital sovereignty debate and the EU-level policy broker, respectively. This rationale for sub-unit selection – or for sampling of context – thus corresponds to the self-explanatory term "extreme case sampling," or to the term "maximum variation sampling," where the selection is motivated by an effort to ensure the widest possible variation within a given dimension (Bryman, 2012, p. 419). Besides variation in terms of expected position within the digital sovereignty debate, the choice of France and the Czech Republic was also motivated by a desire to represent both a larger and a smaller EU Member State, as well as to include both an older and a newer one. However, as the ACF does not expect the views of any government or organization to be homogeneous, it was decided to interview at least three representatives of each of these sub-units and to also investigate the existence of any coalitions within each sub-unit. Furthermore, additional policy participants in the policy subsystem were included to allow for the discovery of the possibility that the hypothesized coalition structure does not correspond to reality. Therefore, interviews were also conducted with informants representing the government of Italy, the private sector, and civil society.

The second major data collection method in this thesis is document analysis (note: here, this term is used interchangeably with the term "content analysis"). In a document analysis in the field of public administration, the researcher studies the content of existing data sources, which consist predominantly of written material, with the aim of understanding and contextualizing the message the author of the document seeks to convey to the audience (van Thiel, 2014). At the same time, a researcher employing data sources that were originally produced for a purpose other than their research project, needs to find and select (only) sources that adequately meet the research needs and use them in such a way that they will "come to concur with the research subject" (van Thiel, 2014, p. 106).

The document analysis referred to in this subsection is distinct from the literature review whose results are presented in chapter 2 (and whose methodology is outlined in section 4.1). Whereas the literature review was predominantly based on peer-reviewed scholarly

literature (i.e., secondary material), the document analysis draws on a set of primary sources which complement the research interviews, and which were mostly recommended or provided to the researcher by the interviewees. This fact supports the requirement of aligning the document selection with the research needs of the project (in fact, these documents can be argued to constitute an "extension" of the data acquired via research interviews). These documents (and other types of artifacts, to be precise) range from national cloud strategies a Power Point presentation summarizing the results of a survey. A full list of these documents, as well as the reasons why each of them was selected for inclusion, can be found in **Appendix C**.

4.3.2 Data Analysis

A rigorous public administration study clearly reports on the data analysis strategy that allowed the researcher to move from raw to ordered data, from ordered data to interpretations, and from interpretations to research findings (Ospina et al., 2018). Raising raw, unstructured data to a conceptual level is often done through the process of coding. Qualitative data analysis techniques resting on coding and retrieving text – techniques which originated in grounded theory (Charmaz, 2006) – are the principal tool of inductive and abductive studies (Bryman, 2012; Timmermans & Tavory, 2012). Coding (also known as indexing) is defined as "deriving and developing concepts from data" (Corbin & Strauss, 2008, p. 3) by breaking the text down into component parts and giving them labels (Bryman, 2012). Coding is an analytical process that requires the researcher to carefully select, interpret, and analyze information without distorting it (Walliman, 2011) – throughout the process, effort is made to preserve the original perspectives of the participants or document authors. The immediate purpose of coding is to create the possibility of comparing data units from different sources or different portions of one source (van Thiel, 2014). Additionally, in some qualitative studies, coding may facilitate theory building (Charmaz, 2006; Walliman, 2011).

In this thesis, both the interview transcripts (and reports) and the analyzed documents were coded using computer-assisted qualitative data analysis software, namely NVivo. Two parallel streams of coding took place – the first one was an open coding process, which started immediately after each interview; the second one followed a predetermined coding frame derived from the main categories of the conceptual framework, and it was only done after a holistic view emerged from the first stream of coding. The second stream of coding formed the basis for the structure of the results (and their discussion) presented in chapter 5. Open and framework-based coding complemented one another well, as the latter provided welcome analytical structure, while the former allowed for the processing of relevant insights which would have fallen though the analytical cracks of the ACF. Nevertheless, the final qualitative synthesis relied almost exclusively on the ACF-based coding frame.

In the second stream of coding, the data was matched with pre-defined categories from the advocacy coalition framework. ACF-based codes were only applied to those portions of the textual material where they were deemed relevant – since all files had already been fully "covered" by the open coding exercise, it was judged acceptable for the second stream of coding to only account for some, but not all passages. As mentioned in section 3.2.1, a coding scheme was created to operationalize the framework. The coding scheme closely reflects all the main concepts of the ACF; it is also informed by some aspects of Jenkins-Smith and Sabatier's (1993) Methodological Appendix. However, while the research design suggested by the authors is quantitative and their coding frame is best suited for longitudinal studies using surveys, the coding scheme developed for the purposes of this thesis – reproduced in **Appendix D** and illustrated in **Appendix F** – is adapted for qualitative coding and a cross-sectional study. As shown in subsections 3.2.2 and 3.2.3, this is consistent with common ways of applying the ACF, where the methods proposed by the authors of the framework are usually not followed literally (Cairney, 2014).

4.3.3 Ensuring the Quality of Research Inquiry

The quality of research and its results is increased when the author pays attention to issues of (1) reliability, (2) replicability, and (3) internal and (4) external validity (Bryman, 2012; Epskamp, 2019; Saunders et al., 2012; van Thiel, 2014). (1) Reliability refers to the degree to which the measures in a study are consistent – in other words, if the procedures involved in the data collection and analysis would yield sufficiently similar results if they were repeated or applied by another researcher (Robson & McCartan, 2016; Saunders et al., 2012). (2) Replicability is ensured when the researcher is transparent enough about the research procedures used in their study for other researchers to be able to follow exactly the same procedures and replicate the study (Bryman, 2012; Epskamp, 2019). (3) Internal validity is achieved when it can be clearly established that claims about causal relationships between independent and dependent variables in the study, hold water (Bryman, 2012). However, in a qualitative, descriptive study such as this one, internal validity is more closely associated with the "appropriateness of the tools, processes, and data" given the research question (Leung, 2015, p. 325). (4) External validity describes the extent to which the findings of the study can be generalized beyond the original research context – e.g., to other relevant social settings or groups (Saunders et al., 2012). Generalizability of the findings of qualitative case studies is typically not an expected attribute, but if the study contains features that render it suitable for meta-syntheses by other researchers, it can be said to satisfy this quality criterion (Leung, 2015).

While scholars have debated about the suitability of these criteria to qualitative research, many interpretivists have still adapted these principles to their research approaches and designs, often – following Guba and Lincoln's seminal work from the 1980s – referring to them under alternative designations such as dependability or confirmability (which parallels reliability and replicability), credibility (as an alternative for internal validity), and transferability (as a qualitative research adaptation of external validity) (Bryman, 2012; Morse et al., 2002; Saunders et al., 2012). While acknowledging this ongoing debate, this thesis will still refer to the more established terms mentioned in the previous paragraph – while making sure not to impose positivist logic where it does not belong. **Appendix K** summarizes some of the measures taken at various stages of writing this thesis to minimize specific threats to the quality of the research inquiry.

4.3.4 Limitations

Nevertheless, after the data collection and analysis stages were completed, it became clear that the methodological design suffered from several limitations, which need to be acknowledged. Firstly, the open coding stage turned out to be mostly superfluous. Due to their open or semi-structured nature, all interviews covered a wide range of topics that were not necessarily relevant to the research objectives of this thesis (an especially common example being organizational and cultural barriers to cloud adoption at the national level). Therefore, the open coding exercise yielded dozens of dead-end codes, which did not correspond well with the ACF-based structure of the results chapter. The open coding stage is still acknowledged in this chapter, as it initially helped the researcher sift through the unstructured data and notice patterns, but it must be admitted that this would have probably happened regardless had only the ACF-based framework been applied.

The second limitation is related to the choice of interview partners. While effort was made to include a range of policy participants – i.e., individuals who are not necessarily government officials –, the decision to focus on an EU-level, public sector-specific policy venue resulted in the fact that the input of the four interview participants familiar with that venue, received disproportionately more attention in the data analysis stage than that of the other interviewees. The two representatives of the private sector in particular provided the researcher with highly useful contextual information, but were not quoted very frequently in the final synthesis (as their input was not as relevant to the core issue), which might have skewed the results too much in the direction of the public sector perspective on the policy problem. Relatedly, the usefulness of interviewing an Italian government representative – i.e., a participant who is not associated with any of the predefined case sub-units – implies that even more accurate insights into the policy problem would have been obtained had the perspective of, for example, Germany or one of the Nordic countries also been included. Nevertheless, limitations on the scope of the work made it impossible to perform more than 13 interviews.

4.4 Ethical Considerations

As this study involved human participants, it is important to address several ethical considerations – "standards of behavior guiding [the researcher's] conduct" in relation to the subjects of their work or other people affected by the work (Saunders et al., 2012, p. 226). In addition, the literature review, the acquisition and analysis of data, and the reporting of findings must be underpinned by the principles of responsibility and honesty. Following Bryman (2012), Saunders et al. (2012), and Walliman (2011), the following steps were taken to ensure the ethical integrity of this study:

- All research subjects (i.e., interviewees) participated voluntarily and were duly informed in advance about the research topic, the research methods, the other sub-units within the case study, and the intended use of the results (including the fact that the author has no intention of publishing or otherwise disseminating the results in any form other than the thesis)

- The interviewees were assured that their identity (i.e., both name and professional title) would be anonymized, so their contribution is not attributable to them personally, and that their personal data (such as contact information) would be managed in full compliance with European data protection legislation

- All interview recordings only started after explicit verbal permission had been secured from the participants; interview recordings were deleted after the submission of the thesis; and interview transcripts will not be retained longer than six months after the thesis submission date

- No harm was done to any research participant (in particular, care was taken not to make any revelations that might compromise the privacy, dignity, or reputation of any individual or organization)

- In no way was any primary data fabricated or deliberately distorted; all secondary sources used in this thesis have been properly acknowledged using the APA (7th edition) citation style; and results have been reported on fully and accurately, even if they might contradict the expected outcomes

- The author is not aware of any conflicts of interest that might have impacted this study

5 Results and Discussion

After analyzing the data yielded by the 13 interviews and the analysis of eight documents provided by the interviewees, it emerged that it is most accurate to group the policy participants into three coalitions (rather than two, as previously assumed based on the literature). This section discusses the policy subsystem, the venue, and the policy problems of interest. Then it describes each of the three coalitions by discussing the policy core beliefs around which they are united, their secondary beliefs (i.e., their beliefs regarding the policy actions that should be undertaken as a reflection of their core policy beliefs), and the membership of the coalition, both at the EU and at the national levels (if applicable). The connection made in the following subsections between policy core beliefs and policy positions, between which the ACF sees a causal relationship, constitutes an element of explanatory research answering the research questions about the factors producing divergence among coalitions. This section ends with a short reflection.

5.1 The Policy Subsystem and the Venue: the MSCCG

The policy subsystem. The policy subsystem in which government cloud computing is discussed in the EU can be split into Member State-level and EU-level policy arenas. As discussed above, there are several important venues within the policy subsystem, such as ENISA's multiple working groups (particularly the one tasked with developing the EUCS) and the private sector-specific working group "Cloud Edge Continuum" of the European Alliance for Industrial Data, Edge and Cloud. However, this thesis focuses on the public sector-specific working group of the Alliance (Participant 8). This working group is known as the informal Member State Cloud Coordination Group (MSCCG) and it consists of representatives of MSs' governments – typically the lead authors of national cloud computing strategies – and the EC. The individuals participating in the group thus have insight into both national-level and EU-level policymaking processes related to government cloud computing, making them extremely valuable sources of information.

The venue. The MSCCG is convened by representatives of the EC's DG CNCT (which is, among other things, responsible for cloud policies under its Future Networks agenda). The MSCCG's inaugural meeting took place on 16 December 2021, and it has been holding biweekly meetings ever since. DG CNCT takes the role of the policy broker, while the Member States represented in the Group are the primary policy actors who, as this thesis argues, can be grouped into coalitions. Nevertheless, the EC's DG DIGIT also often participates in the Group's work as a public sector organization, and many meetings are moderated by the country holding the Presidency of the Council of the EU or by an external rapporteur (Document 1).

5.2 The Policy Problems, the Coalitions, and Their Beliefs

The policy problems. According to Participant 8, one of the main objectives of the Group is to agree on and present to the EC a guidance document with specific criteria for public sector procurement and use of cloud services at all levels of public administration, which will be highly relevant especially for the countries that are currently in the process of developing their eGovernment clouds with the assistance of the Recovery and Resilience Facility funds (which concerns several newer MSs or for example Italy) (Participant 8). This guidance document will cover all the main considerations governments at all levels of administration need to take into account when migrating to the cloud (e.g., when is a data protection impact assessment necessary, with which criteria the chosen service should comply, etc.) (Participant 8). In addition, MSs are discussing ENISA's EUCS (Document 1; Participants 8 & 13) – as a result of these discussions, the EC will adopt the scheme by means of an implementing act, which will lead to the abolition of national-level security schemes such as the French SecNumCloud or the German C5 as all EU MSs will start using the harmonized EU scheme (Participant 8).

The minutes of the meetings offer additional policy problems covered. In the first half of 2022 (under the leadership of the French Presidency), the main subjects over which the MSCCG deliberated included the development of a common vocabulary on data processing services; cloud public procurement; Green Public Procurement; data protection in the cloud; and key principles of cloud security and cybersecurity (Document 1). In the second half of 2022 (after the Czech Presidency took over), the Group has discussed the competition dimension of the CSP market; national experiences with the cloud service switching process (and the issues of interoperability and portability); issues related to procurement (e.g., award criteria and fair market practices); national cloud governance strategies; the development of standard contractual clauses and the ways in which they "should support the negotiating position of public sector bodies as cloud customers" (p. 8); the non-disclosure provisions of cloud computing contracts; or national practices of estimating total cost of ownership in cloud versus on-premise environments (Document 1). (While reading Document 1 might lead one to the conclusion that the focus of the Group shifted slightly from security to market issues as the Presidency changed in July 2022, Participant 11 (a MSCCG member from Italy) does not believe this to be the case.)

An important policy problem for the MSCCG to discuss in order to develop the guidance document for the EC is which "mutually compatible criteria to define trusted cloud services" MSs should agree to mainstream (Document 2, p. 39). In this regard, the French Presidency conducted a particularly insightful survey on the current state of play in national cloud policies in the EU, whose results were presented at one of the early MSCCG meetings (Participants 1, 6, and 8). The purpose of the detailed survey, in which 19 MSs participated, was to serve as a starting point in an effort to establish a common basis for European policies

on cloud computing, and it was discovered that while there are some broad trends, the government cloud landscape in the EU is still quite heterogeneous (Participants 1 and 6). A key conclusion of the survey was that the top priorities in national cloud policies around the EU were modernization and transformation of public action, cybersecurity, cost reduction, and agility (each motivating more than 65% of national policies), while data exploitation and embracing AI, climate change mitigation, and sovereignty played a much smaller role (each being only mentioned in fewer than 30% of national policies) (Document 2). Another crucial finding was the high prevalence of the "cloud first policy" (i.e., the rule that any new information system developed for any government organization should be cloud-based (Participant 2)), embraced by as many as 84% of the participating governments (while in the remaining 16% of national cases, conventional hosting is still an option for public administrations; 18% of MSs have a "public cloud first" policy); of the "cloud first" MSs, 30% additionally have a "SaaS first" policy (Document 2). As for the resources offered to public sector organizations to facilitate the migration to the cloud, 67% of the respondents offer a cloud catalog, but only 27% have a cloud marketplace (Participant 6).

Finally (and most importantly), the survey illuminated the security dimension of national cloud policies in the EU. A key finding is that only 65% of MSs have a classification framework in place for each public sector agency to use to categorize the data it handles (e.g., public, sensitive, strategic, etc. – to correspond with the highly contested EUCS assurance levels) (Document 2; Participant 6). There is broad consensus on the question of data localization – 100% of EU MSs indicated that data and services residency on EU territory is a major concern for them; however, the authors of the survey believe standard contractual clauses (used by 75% of respondents), cybersecurity certification (used by 75%, albeit not in all services), and encryption (58% of cases) are not utilized as frequently as cloud security best practices would necessitate. The French Presidency also incorporated a question in the survey in which MSs were asked whether "providers [being] subject to surveillance of national authorities" was a criterion in the selection of public, GDPR-compliant, trusted, and secure cloud providers, and the answer was affirmative only in 0%, 0%, 14%, and 42% of the cases, respectively (Document 2, p. 30). This fact sets the stage for further exploration of this policy problem – which Participant 8 called *"the only real big elephant in the room"* – from the perspective of different policy actors and coalitions.

5.2.1 Coalition 1: the Proactive Digital Sovereignty Coalition

Policy core beliefs. The main policy core belief of the proactive digital sovereignty coalition is that European cloud solutions are always preferable over non-European ones in the case of government services (especially when it comes to sensitive information), as U.S. CSPs cannot be trusted with EU citizens' personal data, which fall under U.S. legislation (with the CLOUD and FISA Acts being invoked most frequently) (Participants 6, 10, and

13). Participant 6 clearly stated: *"Schrems II and Snowden gave us some food for thought and an opportunity to shift the debate – clearly, we cannot trust American players with personal and business data."* He also adds that some of the European debate on digital sovereignty draws on *"very clever reports explaining that FISA and CLOUD Act pose no risk – reports written by lawyers paid my Microsoft"* (Participant 6). Thus, the members of this coalition believe in the necessity of enacting policies to prevent conflicts of jurisdictions (Participant 6). At the same time, members of this coalition consider it crucial to prioritize efforts to dramatically reduce EU MSs' current dependency on foreign CSPs by building up "a competitive landscape of local players" (Participant 6), albeit recognizing that this will likely take a long time.

Secondary beliefs. The French government's national cloud policy, which was developed relatively recently (in 2021, after a drastic departure from previous policies), rests on three pillars through which the above objectives are to be realized, and France's international position is consistent with its national position (Participants 6 and 10). The three pillars are the spread of security principles associated with the idea of "trusted cloud" (also enshrined in the SecNumCloud label), "cloud at the center" for digitally transforming public administrations (the equivalent of "cloud first"), and a stimulus package for strengthening the domestic industrial base in cloud (Participants 4, 6, and 10). For the purposes of the national government, France is using two internal, inter-ministerial state clouds, which are referred to as "sovereign clouds" (Participants 10 and 13). They are private clouds called Nubo and Pi, operated by the Public Finances Directorate General and the Interior Ministry, respectively, and located on French soil (Participants 10 and 13). Yet, the French government only privileges French companies where necessary – according to Participant 6, 50% of state funds are spent on U.S. technology and 50% on French. *"Our aim is not to eject U.S. technology – they still are best in class,"* Participant 6 explained, adding that there are instances when data flows from the EU to the U.S. are considered acceptable – for example in speech to text software.

At the EU level, France's policy beliefs are translated into efforts to encourage coordination among EU MSs and efforts to boost public and private investment in European cloud infrastructure. EU MS coordination includes pushing for the EUCS to "inherit" many features with SecNumCloud and extending the scope of data falling under assurance level High (Participant 6 was baffled that his European colleagues do not consider this a priority, such as a colleague who thought it was too extreme to consider an IP address to be within the definition of personal data). France is also spreading the idea of "sovereign clouds," which are guaranteed to *"escape application of laws in third country jurisdictions with extraterritorial application, thus preventing EU data being accessed by a third country government,"* for example through a "*capsule of American technology operated by trusted European partners"* (Participant 8) – examples include the partnership between Google and

the French company Thales (Participants 4 and 10). The efforts at deepening EU coordination are interrelated with technological sovereignty and strategic autonomy policies, as evidenced by a statement by the French representative at the MSCCG: The mobilization of common European criteria for trusted cloud services *"will allow the creation of a large market, which is an essential condition for the development and maintenance of a sufficient number of critical size players, which is indispensable for the existence of competitive and quality offers"* (Document 2; Participant 6). These "offers" include both hardware and (Europe's main weakness) software: *"We want to be a software state. You cannot be efficient if you aren't efficient in the production of services"* (Participant 6).

Nevertheless, the key point is that – as strongly expressed by both Participants 8 and 11 – French (and European) capacity to develop alternatives to the world's most popular SaaS applications is nonexistent. One of the participants, who did not wish to be identified in the case of this quote, made a very strong case about this: *"At the MSCCG, we piloted a collaborative tool developed by a German company, and it is working very nicely – I am happy that we are giving the right example – that we are starting to use a European solution, and also to give the company that developed it a bit of a boost. But at the same time – the tool does not function like Microsoft Office 365, it is a completely different level of technology maturity."*

Coalition membership and coordination. The clear leader of this coalition is the government of France. In some questions, France finds an ally in Germany (especially when it comes to spearheading the GAIA-X project). However, Germany's position is more pragmatic and in principle more open to government organizations contracting U.S. CSPs (Participant 10). Therefore, Coalition 1 consists predominantly of one member – as Participant 6 put it: *"There is only one country that believes there is a point in fighting – it is France. (…) Clearly, we are very isolated."* At the EU level, France often invokes the work of the European Data Protection Supervisor and, as mentioned above, the Court of Justice of the EU (and its Schrems I and II judgements, which invalidated the more compromise-seeking positions of the EC) (Participant 6); however, it is a somewhat of a unilateral alignment (two-way cooperation would not be appropriate). That said, on individual policy issues, France is quite successful in finding allies (Participant 6 mentioned a conversation with his Dutch counterparts, who were keen to protect, through trusted and sovereign cloud, the same types of data as France (including, for example, even HR data of – as many others see it – relatively low strategic importance) (Participants 2 and 6). Many of the "neutral" countries of Coalition 3 (see below) share France's policy core beliefs but have different views on the secondary aspects of the policies.

At the French national level, there currently seems to be a surprising degree of consensus on the importance of building up European sovereign clouds, even if it requires significant

government intervention. None of the three French interviewees mentioned any domestic actor opposing the position of Coalition 1. Large domestic CSPs such as OVHcloud or Scaleway are very vocal in both the domestic and the European debates on digital sovereignty and cloud, with the CEOs of these companies at times publicly denouncing the *"lack of ambition and defeatism"* of other European MSs (Participant 10). Other actors shaping the national debate include the Alliance for Digital Trust, which represents digital technology businesses committed to the principles of security, sovereignty, and competitiveness (a vision which they, together with the French government, actively promote at the EU level), or the French section of the pan-European cloud innovation hub EuroCloud (Participants 4, 10, and 13). The main governmental actors shaping the digital sovereignty debate are the Inter-ministerial Directorate for Digital Affairs, which was formed in 2019 to support French public sector agencies in their digital transformation, and the French National Cybersecurity Agency (Participant 13). Using the language of ACF, several internal and external subsystem shocks have contributed to the recently developed position of France. Participant 6 gives an example: *"All French people were traumatized by the Alstom affair – a French senior executive had to spend a year in jail in the U.S* [on corruption charges] *– how did the Department of Justice gather all the information related to the case? After this experience, all French enterprises consider that they need a high level of confidentiality."*

5.2.2 Coalition 2: the Reactive, "Open Strategic Autonomy" Coalition

Policy core beliefs. The second coalition, which may be labelled reactive, is united around the longstanding policy core belief that the U.S. is a trusted political and economic partner and that the benefits which U.S. CSPs can provide to European governments generally outweigh the risks. Therefore, members of this coalition oppose policy measures that draw a line between EU-headquartered service providers and the rest. Representing the position of the Czech government, Participant 1 finds that *"in light of the current events in the Ukraine, it is very strange to lump the U.S. together with Russia or China"* in the European digital sovereignty discourse – a view held especially strongly among policy actors from the newer MSs (as confirmed also by Participants 5 and 12). This position extends to other third countries – Participant 5 emphasized that non-EU countries also include trusted partners such as Canada, South Korea, or Japan, and policies that implicitly view their companies and governments as untrustworthy, are at odds with individual MSs' as well as the EU's foreign policies. In addition, members of this coalition either believe that the risk of U.S. interception of EU citizens' data is negligible, or they do not consider it a grave enough problem when it does happen (Participant 8).

Secondary beliefs. Therefore, one of the main secondary beliefs held by the members of this coalition (and reflected in the policy position they advocate for at the MSCCG) is that

the criteria of the EUCS's assurance level High (or generally the security requirements for technology supporting so-called critical services) should not be as restrictive as advocated for by Coalition 1. Participant 1 considered this the core problem currently being discussed in the MSCCG and summarized his government's official stance as follows: *"The Czech Republic believes that ruling out non-European CSPs from assurance level High would have grave consequences. Three quarters of all Czech governmental cloud-based systems hold citizen data and would be impacted, including 95% of our government HR systems and all agenda management systems used by the government."* Specifically, as explained by Participant 1, while most members of the coalition consider it reasonable to prohibit the storage of EU citizens' data outside of the EU under the EUCS, they are convinced that both backup data and some data necessary for the operation of the cloud services should be permitted to flow to third countries in order to ensure high quality and cybersecurity standards. (In the case of quality, Participant 1 mentioned the example of feeding training data from all over the world into automated translation software; cybersecurity-related examples include the utility of outsourced service desks or the fact that it is in everybody's interest to automatically distribute software updates and patches when a virus or a security flaw are detected.) On the question of the potential conflict between CLOUD Act and GDPR, Participant 1 concedes: *"granted, the U.S. is a global superpower, so it is of course theoretically possible for it to abuse the power, but the primary goal of the law is to fight terrorism."* As if in reaction to Participant 6's mention of the Alstom affair, Participant 1 adds, jokingly: *"if the U.S. finds evidence of corruption among European data, then they are doing European law enforcement agencies a favor, aren't they?"*

Members of Coalition 2 also do not strongly support efforts to build European technological sovereignty, as they have nothing to gain from a very strong French, German, or Italian industry and are thus often skeptical about imposing immunity or sovereignty requirements on cloud services for public sector use (Participant 8). As for the French push for building up European cloud champions, many Coalition 2 members see it as a distortion of internal market competition (Participant 12). Therefore, after extensive consultations with the Confederation of Industry of the Czech Republic and the Ministry of Trade and Industry, the Czech government developed the position that rather than striving for digital sovereignty (a term that should be avoided), the EU should aspire for "open strategic autonomy" (a term also used, for example, in the EC's Strategic Foresight Reports of 2021 and 2022) (Participant 12). The idea is that balance should be sought between the opposing concepts of openness and autonomy. Therefore, the open strategic autonomy model unites the importance of enhancing the resilience of technology supply chains ending in the EU (including by investing in European digital technologies such as AI, 5G, and cloud), with the necessity of open collaboration (and a well-managed interdependence) with Europe's global partners and allies (Participant 12). The context of

this position is clear from both the current Policy Statement of the Government of the Czech Republic and the Program of the Czech Presidency of the Council of the EU – both documents emphasize Europe's transatlantic ties (which the Czech Republic wants to see even further strengthened via the TTC) (Participant 12). Recent EU policy documents where the Czech Republic managed to insert this language during its Council Presidency include the Council Conclusions on the New European Innovation Agenda, where the need to "achieve strategic autonomy while preserving an open economy" is mentioned (Document 8). This view was also articulated by Czech Deputy Prime Minister for Digitalization, Ivan Bartoš, at a conference on digital innovation organized by the Czech presidency in November 2022 – in a break from the agenda of the French presidency, Bartoš and his colleagues stated that EU strategic autonomy must remain open, that technological protectionism should be avoided, and that the EU should deepen its cooperation with the U.S. in the area of digital affairs and standard-setting (Schniderova, 2022; Participant 9). The Czech government also signaled its belief in the need to reconcile strategic autonomy with openness, by hosting the High-level multi-stakeholder event on the Future of the Internet (jointly organized with the EC, and prominently featuring speakers from countries that signed the Declaration on the Future of the Internet, ranging from the U.S. to Japan). The event was an opportunity to reaffirm the country's commitment to the principles of an Internet that is reliable and secure, while being open, free, global, and interoperable (Participant 12).

Coalition membership and coordination. Several Member State governments' official positions are aligned within Coalition 2. According to Participant 9, the Czech Republic informally coordinates its position regarding European digital sovereignty policies with a group of likeminded states known as the Digital Nine Plus (D9+). It is an informal forum of Member States interested – among other things – in pursuing more openness in cross-border data flows, which includes Belgium, the Czech Republic, Denmark, Estonia, Finland, Ireland, Luxembourg, the Netherlands, Poland, Portugal, Spain, and Sweden (Participant 9). Participant 6 (who represents the French government) confirmed that these countries' position is reflected in their behavior in the MSCCG, stating that the Czech Republic and the Nordic countries have especially *"low confidence in the French view on digital sovereignty."* Participant 8, the policy broker at the MSCCG, as well as Participant 11 (of Italy) observed the same divide.

The Member State level is, however, not the only relevant level of analysis – while MS governments adopt official national positions (Documents 5, 6, and 7), those are a result of contestation and debate within the country. For example, the national-level actors in the Czech Republic that have gained a dominant position in shaping the Czech national policy on the question of digital sovereignty and cloud computing include the Confederation of Industry, the Ministry of Trade and Industry, Ministry of Foreign

Affairs, Ministry of the Interior, Office for the Protection of Competition, Prague School of Economics, and several large CSPs including Microsoft and Google (Participants, 1, 5, 7, and 9). These parties regularly coordinate their policy positions in inter-agency meetings, typically led by the Ministry of the Interior. On the other hand, a major Czech policy actor who is more aligned with Coalition 1 is the National Cyber and Information Security Agency (Participants, 1, 5, and 7). According to Participant 5, this Agency is deeply concerned with the extraterritorial effect of U.S. legislation and does believe that European contractual safeguards do not prevent U.S. CSPs from their legal duty to hand in European citizens' data upon request by the authorities. Given its mandate to protect Czech citizens' data and its experience with data breach investigations in countries from Germany to South Korea, the Agency advocates for positions consistent with Coalition 1 and supports the EC's efforts to develop a harmonized EUCS scheme (Participant 5).

5.2.3 Coalition 3: the Relatively Neutral Coalition

Policy core beliefs. The members of the third, relatively neutral coalition emphasize the complexity of the legal and technological situation, which includes many unknowns, and are hesitant to advocate strongly for either Coalition 1's or Coalition 2's position. As Participant 8 put it, the issue of potentially conflicting legal obligations "*is a grey area"* of legal research, where even legal scholars' opinions differ. Alternatively, members of Coalition 3 believe the risk posed by FISA and the CLOUD Act is real, but only on a theoretical level. For example, participant 11, who represents the government of Italy, said that his country shares France's problem perception and concerns about the risk of U.S. surveillance, because the legal possibility exists. *"Today, this is not a real issue. We know there have been very few cases when this happened. But from a legal point of view, our administrations are afraid. If this happens, who will be responsible? This is a typical way Napoleonian states like Italy or France usually think. This is why we are aligned in terms of our theoretical approach."* Nevertheless, from a practical point of view, Participant 11 finds the French approach *"too idealistic"* in its efforts to build European alternatives to U.S. hyperscalers, as this cannot be achieved in the short term – *"there is no such market in Europe. (…) And we will not have a European cloud for the next 10 years."* Similarly, Participant 8 wondered if larger MSs' initiatives to develop European tech alternatives might go *"against even their understanding of what could be logically achieved."* While recognizing the need to build European tech champions, members of Coalition 3 see European strategic autonomy as "*a separate issue"* (Participant 11), and a long-term one.

However, unlike Coalition 2, Coalition 3 does not tend to accuse Coalition 1 of unfair market practices. Speaking from his perspective as the policy broker within the policy venue, Participant 8 offered his take: *"Larger MSs have a larger appetite to battle the issue and also function as a convening power – saying, let's bring all the European MSs together*

and let's find alternatives. Smaller MSs sometimes suspect that this is coming out of motives of pushing standards of larger European MSs on the market to benefit their own cloud industries over the SME industries, for example, of smaller MSs." As discussed above, one of the main policy problems where this plays out is the debate about the candidate EUCS, where the possible inclusion of criteria of immunity to non-EU laws or absence of third country ownership is being discussed, where Coalition 2 diverges the most from the positions of larger MSs. Participant 8 continued: *"To better grasp that conflict, I ask myself – do I see a way for a larger EU MS to actually push market standards to benefit their own industry over smaller EU MS? I do not"* – adding that France has also been promoting small CSPs from countries such as Estonia, who would otherwise not have sufficient exposure among public sector organizations in EU Member States.

Secondary beliefs. The secondary aspects of the relatively neutral countries' positions vary and attempting to provide a comprehensive overview is outside the scope of this thesis. However, Italy's approach can be discussed as an example. Participant 11 understands digital sovereignty as a country's right over its own data, which should not be accessible by a third country through a warrant – a fundamentally legal problem. Thus, it makes limited sense to respond to the challenges posed by FISA and the CLOUD Act primarily through technical solutions and strategic autonomy measures. At the same time, he believes attempts to put pressure on the U.S. through digital sovereignty measures in the hope that Washington will change the legislation (so its tech companies do not lose access to the EU market) are unlikely to be successful. Instead, *"it is about trying to find a way to "hack" the legal basis that allows a third country to access the data"* (Participant 11). In his view (and by extension that of the Italian government), hacking the legal basis amounts to having a local company manage the cloud infrastructure on which U.S. technology and software is deployed – in Italy's understanding, if the U.S. company does not own the infrastructure, the U.S. government cannot legally claim any data (Participant 11). Thus, one of the pillars of the Italian cloud strategy has been the creation of the National Strategic Hub – *"a national infrastructure for the provision of cloud services, whose management and control are independent from non-EU providers"* (Document 7). The operator of this sovereign cloud infrastructure is a newly created Italian company, which will – as defined by the tender – offer public cloud services (using the technology of Google Cloud, AWS, Microsoft, Oracle, etc.) to all interested Italian public administrations (Participant 11).

Participant 8 also describes that many MSs set aside the *"rules-based concern centered on conflicting legal obligations"* and focus on the practical matters. More practically oriented policy actors adopt the common European approach of requiring companies to take legal, organizational, and technical measures to prevent potentially unlawful access to data. According to Participant 8, one such technical measure, popular among pragmatic

organizations, is encryption – *"with offsite decryption key storage, the CSP cannot access the decryption key"* and accommodate a data access request from the authorities, even if they wanted to comply (Participant 8). The possibility of two-way encryption is also consistently brought up by large private sector players (Participants 4 and 9). On the other hand, some MSs conclude that irrespective of FISA and the CLOUD Act, "*U.S. agencies already have ways to enter and access data which is of interest to them"* and thus see limited sense in trying to avoid using U.S.-headquartered CSPs at all costs. The way different countries approach this issue may thus also depend on their cultures and administrative traditions, with more legalistic countries paying more attention to the legal dimension and perhaps not asking themselves whether *"the NSA has ways to crack encryption"* with their supercomputer (Participant 8).

Coalition membership and coordination. As discussed above, the relatively neutral group of stakeholders is quite loose and does not engage in coordinated activity per se. The policy broker of the MSCCG, a representative of DG CNECT, also belongs here – not by definition (it is not assumed that policy brokers are always impartial), but due to the opinions he voiced. At the EU level, this coalition is said to comprise of countries such as Germany, Italy, and Spain. At a lower level of administration in all countries, there are many actors who are aligned with Coalition 3, including many companies (Participant 4).

The European Commission – here as a public sector organization rather than an intergovernmental body – is an interesting example of an actor that gives "partial credit" to Coalition 1's belief that EU CSPs are generally preferrable. According to Participant 2, the EC has contracts with four CSPs – mostly AWS Microsoft, and IBM, but also OVHcloud. Participant 3, who was responsible for deciding on which CSP to contract for several EC projects and use cases, reflected on the reasoning behind his choices. For a large geospatial database, AWS was chosen *"because it was easiest to set up"* when the decision was made to decouple the database from the EC's physical infrastructure (so as to improve uptime, security, and scalability) – in his experience, the most mature and sophisticated products with the best customer support, are offered by the hyperscalers. However, for a smaller-scale, experimental project for testing a data sharing technology (in a containerized stack for APIs), OVHcloud was selected because Participant 3 wanted to use an EU provider. Nevertheless, the "price" he had to pay for using OVHcloud was the fact that setting up the solution required more technical knowledge on the part of the user, that there turned out to be bugs in the code, and that some of the documentation was only available in French (Participant 3). This testifies to the fact that gaps between the quality of European versus U.S. CSPs persist, and that some organizations are nevertheless willing to experiment with European solutions due to individual actors' belief in the necessity of boosting European technological sovereignty.

5.3 Reflection

The MSCCG of the European Alliance for Industrial Data, Edge and Cloud is a fascinating policy forum for EU Member States' top experts on government clouds to exchange their views and find ways to solve their common problems. On the level of large government organizations, a unified institutional approach to cloud procurement has proven to increase the government's leverage vis-à-vis CSPs – from various government-wide dynamic purchasing systems (Participant 7) to cloud contract brokerage, a function DG DIGIT performs behalf of other DGs and EU institutions in order to use bulk purchases as a way to negotiate not only on better prices, but also on stronger legal and security aspects (Participant 2).

Coordination of national cloud strategies among EU Member States extends this logic to a continent-wide level. The EUCS and other EU initiatives are going to make cloud procurement at all levels of administration more streamlined, as it is currently difficult for public sector organizations to navigate the complexity of different CSPs' security approaches, but also the diversity of contracts CSPs offer, often charging different organizations different prices for the same service (Participant 11). After the three coalitions outlined in the previous section agree on key questions such as the requirements for different assurance levels and compatible ways of categorizing data, the EUCS is expected to be finalized within a year (Participant 11). While none of the interviewees dared to estimate what compromise solution the group is most likely to reach (noting, too, that the MSCCG is not the only forum where the scheme is being discussed), all of them were confident that one will be found.

A problem that seems likely to remain, as no amount of Member State coordination will solve it anytime soon, is the SaaS problem. As explained by Unnamed participant, while at the lower levels of the cloud stack there are more opportunities for competition, Microsoft Office 365's absolute dominance in the office suite market is unlikely to be challenged by any viable competitor in the foreseeable future. The issue with SaaS products is that it is not technically feasible to effectively safeguard the data in transit with double key encryption – not for a large volume of data such as those supporting Office 365 users' activity – activity that may generate very valuable personal data (Unnamed participant). The European Commission's institutional use of Office 365 has been investigated by the EU Data Protection Supervisor; the German data protection authorities consider Microsoft's telemetry to be breaching the GDPR (Unnamed participant). So far, there does not appear to be a satisfactory solution to this problem, but fortunately it is up next on the MSCCG's agenda.

6 Conclusion

This thesis investigated the advocacy coalitions shaping the European digital sovereignty debate related to cloud computing. To answer the first research sub-question about the ways in which European digital sovereignty considerations are reflected in public sector cloud policies, the core problem was first outlined – the extraterritorial reach of two key pieces of U.S. legislation, namely FISA Act and CLOUD Act, which enable U.S. law enforcement authorities to request access to European citizens' data in the possession of CSPs headquartered in the U.S. It was shown that the European digital sovereignty policies that seek to ameliorate this problem include long-term (strategic autonomy) measures to strengthen European cloud alternatives through investment, infrastructure federation, and European interoperability standards, and short-term measures such as harmonized cloud certification schemes, the mainstreaming of EU-approved standard contractual clauses requiring CSPs to take legal, organizational, and technical measures to fend off Washington's data disclosure requests (and to be transparent whenever such requests are received), and EU-led capacity building and coordination among MSs.

The second research sub-question investigated the main points of disagreement among the stakeholders formulating and implementing these policies. It was shown that the long-term strategic autonomy measures are often accused of being a guise for larger MSs' protectionist policies, which might harm the EU cloud market; proposed cloud certification schemes with data localization and "sovereignty requirements" are likewise criticized for entailing unacceptable market and cybersecurity tradeoffs. Thereafter, building on Baischew et al. (2020), it was proposed that the critical position is mainly adopted by smaller MSs (labeled "reactive"), while the purportedly techno-nationalist stance is associated with larger MSs, especially Germany and France (labeled "proactive" actors). This tentative division set the stage for the empirical part, which answered the third sub-question – one seeking to uncover the main factors producing this divergence among MSs.

The empirical part of this thesis consisted of a series of in-depth expert interviews targeting EU and national-level cloud experts, including those participating in the informal MSs' Cloud Cooperation Group, which is at the epicenter of the European debate on digital sovereignty and government clouds. Based on insights from these interviews, the advocacy coalition framework was used to sketch a map of the advocacy coalitions that have emerged in the debate; the "factors producing this divergence" are associated with ACF's relationship between coalitions' policy core beliefs and secondary beliefs (i.e., differentiated beliefs and problem perceptions shape the diverging policies advocated by each coalition).

Thus, this thesis concludes that the structure of the advocacy coalitions shaping the debate on European digital sovereignty and cloud, which builds on but modifies the tentative twofold division based on the literature, can be briefly described as follows. The proactive digital

sovereignty coalition, consisting solely of France and occasionally of Germany, sees it as a major problem when a foreign jurisdiction can unlawfully access EU citizen data, both as a matter of principle and for strategic, economic, and security reasons. It also believes that the U.S. government actively works to acquire EU data on the basis of FISA and CLOUD Act. These beliefs are translated into efforts to establish and spread sovereign and trusted cloud labels with data localization requirements, which would render non-EU CSPs ineligible for many contracts involving sensitive data. Simultaneously, this coalition seeks to radically speed up the development of EU CSPs, including via public investment. The second coalition is the reactive group, which unites newer MSs and the Nordic countries and advocates for European strategic autonomy to remain "open" to collaboration with third countries. The policy core beliefs motivating this group include the importance of transatlantic ties and the position that while U.S. legislation might enable the government to access EU citizens' data through warrants directed at U.S.-headquartered CSPs, the risk of this happening at a scale that might raise concerns, is extremely low. Simultaneously, these countries have relatively well-established eGovernment clouds taking advantage of the best-in-class market offerings, and do not see a good enough reason to give this up. Thus, this coalition opposes criteria in future cloud cybersecurity schemes that restrict third country players' access and does not see public investment in European tech champions as a priority. The third, relatively neutral coalition of the remaining MSs either does not have a strong theory on the way U.S. legislation should be interpreted or acknowledges the theoretical legal possibility of data interception but does not consider this a practically relevant issue. In contrast to the reactive coalition, the neutral coalition does not accuse France of nefarious tech expansionism but considers efforts to build EU alternatives to U.S. hyperscalers naïve. Therefore, the national cloud strategies of these players seek ways to take advantage of U.S. offerings while putting in place measures to circumvent potential extraterritorial legislation, such as by procuring U.S. infrastructure and software but making sure a domestic company is the formal owner. This group's collaboration with U.S. partners is not as strong on a political and diplomatic level. Meanwhile, the coalition thinks European technological sovereignty and strategic autonomy should be built, but gradually.

6.1 Future Research

Taking advantage of the features of the ACF, which enable longitudinal studies tracing policy change, papers building on this thesis could investigate whether the coalitions described in this thesis remain stable. They could also compare the relative power and policy influence of the respective coalitions by systematically linking future policy outcomes with coalition positions and measuring their success (the finalized EUCS would be one such candidate). Finally, future research should delve deeper into the positions of MSs that this thesis assumes belong to the relatively neutral coalition, to see if their national cloud strategies really place them there. Lastly, future studies could investigate the effect of subsystem shocks such as cyberattacks or hacks, on coalition membership.

Reference List

Abied, O., Ibrahim, O., & Mat Kamal, S. N.-I. (2022). Adoption of Cloud Computing in E-Government: A Systematic Literature Review. *Pertanika Journal of Science and Technology*, *30*(1), 655–689. https://doi.org/10.47836/pjst.30.1.36

Adonis, A. A. (2019). Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy. *Global: Jurnal Politik Internasional*, *21*(2), 262. https://doi.org/10.7454/global.v21i2.412

Al Ghaffar, H. A. (2020). Government Cloud Computing and National Security. *Review of Economics and Political Science*, *ahead-of-p*(ahead-of-print). https://doi.org/10.1108/reps-09-2019-0125

Ali, O., Shrestha, A., Osmanaj, V., & Muhammed, S. (2021). Cloud computing technology adoption: an evaluation of key factors in local governments. *Information Technology and People*, *34*(2), 666–703. https://doi.org/10.1108/ITP-03-2019-0119

Almarabeh, T., Majdalawi, Y. K., & Mohammad, H. (2016). Cloud Computing of E-Government. *Communications and Network*, *08*(01), 1–8. https://doi.org/10.4236/cn.2016.81001

Altmann, J., & Aryal, R. G. (2020). Refinement of Cost Models for Cloud Deployments through Economic Models Addressing Federated Clouds. In T. Lynn, J. G. Mooney, P. Rosati, & G. Fox (Eds.), *The Business Value of Cloud Computing* (pp. 73–88). Palgrave Macmillan. http://www.palgrave.com/gp/series/16004

Andreas, A., Mavromoustakis, C. X., Mastorakis, G., Do, D. T., Batalla, J. M., Pallis, E., & Markakis, E. K. (2021). Towards an optimized security approach to IoT devices with confidential healthcare data exchange. *Multimedia Tools and Applications*, *80*(20), 31435–31449. https://doi.org/10.1007/s11042-021-10827-x

Baezner, M. (2018). *Trend Analysis: Cyber Sovereignty and Data Sovereignty*.

Baischew, D., Kroon, P., Lucidi, S., Märkel, C., & Sörries, B. (2020). *Digital sovereignty in Europe: A first benchmark*. https://www.econstor.eu/handle/10419/251539

Baltrusaitis, J. (2022). *Amazon AWS accounts for 33% of the global cloud infrastructure service market*. Finbold. https://finbold.com/amazon-aws-statistics/

Barrinha, A., & Christou, G. (2022). Speaking sovereignty: the EU in the cyber domain. *European Security*, *31*(3), 356–376. https://doi.org/10.1080/09662839.2022.2102895

Becerra, M., & Waisbord, S. R. (2021). The curious absence of cybernationalism in Latin America: Lessons for the study of digital sovereignty and governance. *Communication and the Public*, *6*(1–4), 67–79. https://doi.org/10.1177/20570473211046730

Beim, J. (2018). Enforcing a Prohibition on International Espionage. *Chicago Journal of International Law*, *18*(2).

Bertuzzi, L. (2022). Is data localization coming to Europe? *Iapp*. https://iapp.org/news/a/is-data-localization-coming-to-europe/

Beyers, J., & Kerremans, B. (2004). Bureaucrats, politicians, and societal interests: How is European policy making politicized? *Comparative Political Studies*, *37*(10), 1119–1150. https://doi.org/10.1177/0010414004269828

Biswash, S. K., & Jayakody, D. N. K. (2020). A fog computing-based device-driven mobility management scheme for 5G networks. *Sensors (Switzerland)*, *20*(21), 1–19. https://doi.org/10.3390/s20216017

Bodó, B., Irion, K., Janssen, H., & Giannopoulou, A. (2021). Personal data ordering in context: The interaction of meso-level data governance regimes with macro frameworks. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1581

Braud, A., Fromentoux, G., Radier, B., & Le Grand, O. (2021). The Road to European Digital Sovereignty with Gaia-X and IDSA. *IEEE Network*, *35*(2), 4–5. https://doi.org/10.1109/MNET.2021.9387709

Brooks, E. (2018). Using the Advocacy Coalition Framework to understand EU pharmaceutical policy. *European Journal of Public Health*, *28*, 11–14. https://doi.org/10.1093/eurpub/cky153

Bryman, A. (2012). *Social Research Methods* (4th Editio). Oxford University Press.

Buavirat, W., Kreesuradej, W., & Chaveesuk, S. (2019). The framework of government cloud computing adoption with TAM in Thailand. *ACM International Conference Proceeding Series*, 196–200. https://doi.org/10.1145/3357419.3357458

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, *21*(5), 594–613. https://doi.org/10.1177/1367549417751151

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, *42*(3), 391–413. https://doi.org/10.1080/13523260.2021.1907129

Burwell, F. (2020). US-EU relations: A post-covid transatlantic digital agenda. In C. Hobbs (Ed.), *Europe's Digital Sovereignty: From rulemaker to superpower in the age of US-China rivalry* (pp. 44–53). European Council on Foreign Relations. https://www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf

Büttner, S. M., Leopold, L., Mau, S., & Posvic, M. (2015). Professionalization in EU Policy-Making? The topology of the transnational field of EU affairs. *European Societies*, *17*(4), 569–592. https://doi.org/10.1080/14616696.2015.1072229

Cairney, P. (2014). *Paul A. Sabatier, "An Advocacy Coalition Framework of Policy Change and the Role of Policy-Oriented Learning Therein."* 484–497.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: the false promise of digital sovereignty? *European Security*, *31*(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Calzati, S. (2022). "Data sovereignty" or "Data colonialism"? Exploring the Chinese involvement in Africa's ICTs: a document review on Kenya. *Journal of Contemporary African Studies*, *40*(2), 270–285. https://doi.org/10.1080/02589001.2022.2027351

Campbell, R., Goodman-Williams, R., Feeney, H., & Fehler-Cabral, G. (2020). Assessing Triangulation Across Methodologies, Methods, and Stakeholder Groups: The Joys, Woes, and Politics of Interpreting Convergent and Divergent Data. *American Journal of Evaluation*, *41*(1), 125–144. https://doi.org/10.1177/1098214018804195

Caravella, S., Costantini, V., & Crespi, F. (2021). Mission-oriented policies and technological sovereignty: The case of climate mitigation technologies. *Energies*, *14*(20). https://doi.org/10.3390/en14206854

Carullo, G., & Ernst, C. (2020). Data Storage by Public Administrations. *European Public Law*, *26*(3), 545–568.

Catteddu, D. (2010). *Security & Resilience in Governmental Clouds: Making an Informed Decision - A Report by ENISA*.

Celeste, E. (2021). Digital Sovereignty in the EU: Challenges and Future Perspectives. In F. Fabrini, E. Celeste, & J. Quinn (Eds.), *Data Protection Beyond Borders* (Issue February). https://doi.org/10.5040/9781509940691.ch-013

Celeste, E., & Fabbrini, F. (2021). Competing Jurisdictions: Data Privacy Across the Borders. *Palgrave Studies in Digital Business and Enabling Technologies*, 43–58. https://doi.org/10.1007/978-3-030-54660-1_3

CEO Roundtable Members. (2021). *European industrial technology roadmap for the next generation cloud-edge offering*. *May*. https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf

Chandran, R., & Davydova, A. (2022). Behind Russia's "digital iron curtain", tech workarounds thrive. *Reuters*. https://www.reuters.com/legal/litigation/behind-russias-digital-iron-curtain-tech-workarounds-thrive-2022-03-23/

Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. SAGE Publications.

Chenou, J. M., & Radu, R. (2019). The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union. *Business and Society*, *58*(1), 74–102.

https://doi.org/10.1177/0007650317717720

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.

Codagnone, C., Liva, G., Gunderson, L., Misuraca, G., & Rebesco, E. (2021). *Europe's Digital Decade and Autonomy*.

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*(1), 104–126. https://doi.org/10.1007/BF03177550

Corbin, J., & Strauss, A. (2008). Strategies for Qualitative Data Analysis. In S. Publications (Ed.), *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory* (pp. 65–86). https://doi.org/10.4135/9781452230153.n4

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

Csernatoni, R. (2022). The EU's hegemonic imaginaries: from European strategic autonomy in defence to technological sovereignty. *European Security*, *31*(3), 395–414. https://doi.org/10.1080/09662839.2022.2103370

Daly, A. (2016). Dominance and the Cloud. In *Private Power, Online Information Flows and EU Law: Mind the Gap* (pp. 120–136). Hart Publishing. https://doi.org/<http://dx.doi.org/10.5040/9781509900664.ch-006

Daucé, F., & Musiani, F. (2021). Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: An introduction. *First Monday*, *26*(5). https://doi.org/10.5210/fm.v26i5.11685

De Filippi, P. (2013). Foreign clouds in the european sky: How US laws affect the privacy of europeans. *Internet Policy Review*, *2*(1), 1–7. https://doi.org/10.14763/2013.1.113

De Gregorio, G., & Radu, R. (2022). Digital constitutionalism in the new era of Internet governance. *International Journal of Law and Information Technology*, *30*(1), 68–87. https://doi.org/10.1093/ijlit/eaac004

de Hert, P., & Thumfart, J. (2021). The Microsoft Ireland case, the CLOUD Act and the cyberspace sovereignty trilemma. In W. Hötzendorfer, C. Tschohl, & F. Kummer (Eds.), *International trends in legal informatics* (pp. 373–417). Nova MD. https://doi.org/10.38023/47fd0a3f-c62a-4cd6-840e-e8ea89bdea68

de La Bruyère, E., & Picarsic, N. (2020). *China Standards 2035: Beijing's Platform Geopolitics and "Standardization Work in 2020."* www.horizonadvisory.org

DIGITALEUROPE. (2022). *Joint letter on "sovereignty requirements" in candidate European Cybersecurity Certification Scheme for Cloud Services*. https://digital-europe-website-v1.s3.fr-par.scw.cloud/uploads/2022/06/DIGITALEUROPE_Joint-letter-on-'sovereignty-requirements-in-candidate-EUCS.pdf

Drezner, D. W. (2019). Technological change and international relations. *International Relations*, *33*(2), 286–303. https://doi.org/10.1177/0047117819834629

Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). New Public Management Is Dead - Long Live Digital-Era Governance. *Journal of Public Administration Research and Theory*, *16*(3), 467–494. https://doi.org/10.1093/jopart/mui057

El-Gazzar, R., Hustad, E., & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A Delphi study approach. *Journal of Systems and Software*, *118*, 64–84. https://doi.org/10.1016/j.jss.2016.04.061

ENISA. (2020). *EUCS – Cloud Services Scheme: A candidate cybersecurity certification scheme for cloud services* (Issue December). https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme

Epifanova, A. (2020). Deciphering Russia's " Sovereign Internet Law " Tightening Control and Accelertaing the Splinternet. *Ssoar*, *2*, 0–11. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-66221-8

Epskamp, S. (2019). Reproducibility and Replicability in a Fast-Paced Methodological World.

Advances in Methods and Practices in Psychological Science, *2*(2), 145–155. https://doi.org/10.1177/2515245919847421

Esposito, C., Castiglione, A., & Choo, K. K. R. (2016). Encryption-Based Solution for Data Sovereignty in Federated Clouds. *IEEE Cloud Computing*, *3*(1), 12–17. https://doi.org/10.1109/MCC.2016.18

Esposito, C., Castiglione, A., Frattini, F., Cinque, M., Yang, Y. J., & Choo, K. K. R. (2019). On Data Sovereignty in Cloud-Based Computation Offloading for Smart Cities Applications. *IEEE INTERNET OF THINGS JOURNAL*, *6*(3), 4521–4535. https://doi.org/10.1109/JIOT.2018.2886410

EU Member States. (2020). *Declaration: Building the next generation cloud for businesses and the public sector in the EU*. https://digital-strategy.ec.europa.eu/en/news/towards-next-generation-cloud-europe

European Commission. (2020). A European Strategy for Data. *European Commission*, (2020) COM/2020/66 final.

European Commission. (2022a). *Chips Act - Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem* (p. COM(2022) 46 final).

European Commission. (2022b). *Cyber Resilience Act: Regulation of the European Parliament and the Council on horizontal cybersecurity requirements for products with digital elements* (p. COM(2022) 454 final). https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

European Commission. (2022c). *Data Act: the Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data* (p. COM(2022) 68 final). https://doi.org/10.2139/ssrn.4110462

European Commission. (2022d). Data Governance Act: Regulation 2022/868 of the European Parliament and of the Council. *Official Journal of the European Union*, *2022*(April), 1–44.

European Commission. (2022e). *European Declaration on Digital Rights and Principles for the Digital Decade* (p. COM(2022) 28 final).

European Commission. (2022f). *Proposal for an Artificial Intelligence Act* (p. COM(2021) 206 final).

European Commission. (2022g). *Report on the monitoring of the Berlin Declaration* (Issue May). https://www.numerique.gouv.fr/uploads/20220506_Berlin_Declaration_monitoring_report_2022.pdf

European Commission. (2022h). *Standard Contractual Clauses (SCC): Standard contractual clauses for data transfers between EU and non-EU countries*. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

European Economic and Social Committee. (2021). *Digital Services Act and Digital Markets Act: Stepping stones to a level playing field in Europe*. 1–2. https://doi.org/10.2864/74293

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Federal Register. (2020). *Executive Order 13942: Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain*. *85*(155), 48637–48639. https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency

Ferrer, A. J., Pérez, D. G., & González, R. S. (2016). Multi-cloud Platform-as-a-service Model, Functionalities and Approaches. *Procedia Computer Science*, *97*, 63–72. https://doi.org/10.1016/j.procs.2016.08.281

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy and Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Gaia-X. (2022). *Who are we?* https://gaia-x.eu/who-we-are/association/

German Presidency of the Council of the EU. (2020). *Berlin Declaration on Digital Society and Value-Based Digital Government*.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2022). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *00*(00), 1–40.

Goldacker, G. (2017). Digitale Souveränität. In *Handbuch Digitalisierung in Staat und Verwaltung*. https://doi.org/10.1007/978-3-658-23669-4_21-1

Gregor, S. (2006). The nature of theory in Information Systems. *MIS Quarterly*, *30*(3), 611–642. http://heim.ifi.uio.no/~petterog/Kurs/INF5220/NatureofTheoryMISQ.pdf

Gstrein, O. J., & Zwitter, A. J. (2021). Extraterritorial application of the GDPR: Promoting european values or power? *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1576

Gueham, F. (2017). Digital Sovereignty – Steps Towards a New System of Internet Governance. *The Fondation Pour l'innovation Politique*, *January*. https://euagenda.eu/publications/digital-sovereignty-steps-towards-a-new-system-of-internet-governance

Haeberlen, T., Liveri, D., & Lakka, M. (2013). *Good Practice Guide for Securely Deploying Governmental Clouds*. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/good-practice-guide-for-securely-deploying-governmental-clouds

Halkias, D., Neubert, M., Thurman, P. W., & Harkiolakis, N. (2022). The Multiple Case Study Design: Methodology and Application for Management Education. In *The Multiple Case Study Design*. Rout.

Hildén, J. (2021). Mitigating the risk of us surveillance for public sector services in the cloud. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1578

Hummel, P., Braun, M., & Dabrock, P. (2019). Data Donations as Exercises of Sovereignty. In *Philosophical Studies Series* (Vol. 137). https://doi.org/10.1007/978-3-030-04363-6_3

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

Husovec, M., & Roche Laguna, I. (2022). Digital Services Act: A Short Primer. In M. Husovec & I. Roche Laguna (Eds.), *Principles of the Digital Services Act*. Oxford University Press. https://doi.org/10.2139/ssrn.4153796

Information Technology Industry Council. (2022). *European Cybersecurity Certification Scheme for Cloud Services*. https://www.itic.org/documents/europe/Final_EUCS_statement_1406.pdf

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

ISO. (2014). *International Standard ISO/IEC 17788: Information technology — Cloud computing — Overview and vocabulary* (Vol. 2014).

ISO. (2015). *ISO/IEC 27017:2015, Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*.

Jang, S., Weible, C. M., & Park, K. (2016). Policy processes in South Korea through the lens of the Advocacy Coalition Framework. *Journal of Asian Public Policy*, *9*(3), 274–290. https://doi.org/10.1080/17516234.2016.1201877

Jenkins-Smith, H., & Sabatier, P. (1993). Methodological Appendix: Measuring Longitudinal Change in Elite Beliefs Using Content Analysis of Public Documents. In P. Sabatier & H. Jenkins-Smith (Eds.), *Policy Change and Learning: An Advocacy Coalition Approach* (pp. 237–256). Westview Press.

Johansson, B., & Ruivo, P. (2013). Exploring Factors for Adopting ERP as SaaS. *CENTERIS 2013 - HCIST 2013 - International Conference on Health and Social Care Information Systems and Technologies*, *9*, 94–99. https://doi.org/10.1016/j.protcy.2013.12.010

Jones, S., Irani, Z., Sivarajah, U., & Love, P. E. D. (2019). Risks and rewards of cloud computing in the UK public sector: A reflection on three Organisational case studies. *Information Systems Frontiers*, *21*(2), 359–382. https://doi.org/10.1007/s10796-017-9756-0

Kabelka, L. (2022). Sovereignty requirements remain in cloud certification scheme despite backlash. *Euractiv*. https://www.euractiv.com/section/cybersecurity/news/sovereignty-requirements-remain-in-cloud-certification-scheme-despite-backlash/

Kaloudis, M. (2021). Digital sovereignty–European Union's action plan needs a common understanding to succeed. *History Compass*, *19*(12), 1–12. https://doi.org/10.1111/hic3.12698

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. In *Technical report, Ver. 2.3 EBSE Technical Report. EBSE*.

Knutsson, H. (2017). Advocacy Coalition Learning: Biases and Heuristics in Policy Implementation. *Statsvetenskaplig Tidskrift*, *119*(1), 163–183.

Koch, D. J., & Burlyuk, O. (2019). Bounded policy learning? EU efforts to anticipate unintended consequences in conflict minerals legislation. *Journal of European Public Policy*. https://doi.org/10.1080/13501763.2019.1675744

Kuan Hon, W., Millard, C., & Walden, I. (2012). Negotiating cloud contracts: looking at clouds from both sides now. *Standard Technology Law Review*, *16*(1), 245–255.

Kushwaha, N., Roguski, P., & Watson, B. W. (2020). Up in the Air: Ensuring Government Data Sovereignty in the Cloud. *International Conference on Cyber Conflict, CYCON*, *2020-May*, 43–61. https://doi.org/10.23919/CyCon49761.2020.9131718

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

Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review*, *22*(3), 482–506. https://doi.org/10.1093/isr/viz022

Lambach, D., & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. *Governance*, *October 2021*, 1–17. https://doi.org/10.1111/gove.12690

Lantis, J. S., & Bloomberg, D. J. (2018). Changing the code? Norm contestation and US antipreneurism in cyberspace. *International Relations*, *32*(2), 149–172. https://doi.org/10.1177/0047117818763006

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers and Security*, *72*, 26–59. https://doi.org/10.1016/j.cose.2017.08.005

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324. https://doi.org/10.4103/2249-4863.161306

Li, H., & Yang, X. (2021). Sovereignty and Network Sovereignty. In *Co-governed Sovereignty Network*. Springer. https://doi.org/10.1007/978-981-16-2670-8

Liang, Y., Qi, G., Wei, K., & Chen, J. (2017). Exploring the determinant and influence mechanism of e-Government cloud adoption in government agencies in China. *Government Information Quarterly*, *34*(3), 481–495. https://doi.org/10.1016/j.giq.2017.06.002

Liang, Y., Qi, G., Zhang, X., & Li, G. (2019). The effects of e-Government cloud assimilation on public value creation: An empirical study of China. *Government Information Quarterly*, *36*(4), 101397. https://doi.org/10.1016/j.giq.2019.101397

Lundell, B., Gamalielsson, J., & Katz, A. (2020). Addressing lock-in effects in the public sector: How can organisations deploy a saas solution while maintaining control of their digital assets? *CEUR Workshop Proceedings*, *2797*, 289–296.

Lynn, T., Rosati, P., & Fox, G. (2020). Measuring the Business Value of Cloud Computing: Emerging Paradigms and Future Directions for Research. In T. Lynn, J. G. Mooney, P. Rosati, & G. Fox (Eds.), *The Business Value of Cloud Computing* (pp. 107–121). Palgrave Macmillan. http://www.palgrave.com/gp/series/16004

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data and Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Mainwaring, S. (2020). Always in control? Sovereign states in cyberspace. *European Journal of*

International Security, *5*(2), 215–232. https://doi.org/10.1017/eis.2020.4

Mann, M., & Daly, A. (2019). (Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism. *Television and New Media*, *20*(4), 379–395. https://doi.org/10.1177/1527476418806091

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian internet policy. *Media and Communication*, *5*(1), 29–41. https://doi.org/10.17645/mac.v5i1.808

Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. In *International Review of the Red Cross*. https://doi.org/10.1017/S1816383122000194

Masood, A., & Hashmi, A. (2019). AIOps: Predictive Analytics & Machine Learning in Operations. In *Cognitive Computing Recipes* (pp. 359–382). Apress. https://doi.org/10.1007/978-1-4842-4106-6_7

Maurer, T., Morgus, R., Skierka, I., & Hohmann, M. (2015). Technological sovereignty: Missing the point? *International Conference on Cyber Conflict, CYCON*, *2015-Janua*(November 2014), 53–67. https://doi.org/10.1109/CYCON.2015.7158468

McGillivray, K. (2022). *Government Cloud Procurement: Contracts, Data Protection, and the Quest for Compliance*. Cambridge University Press.

Mell, P., & Grance, T. (2012). The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology. *Public Cloud Computing: Security and Privacy Guidelines*, 97–101.

Moerel, L., & Timmers, P. (2021). Reflections on Digital Sovereignty. *Research in Focus, January*. https://eucyberdirect.eu/research/reflections-on-digital-sovereignty

Mohammed, F., Ibrahim, O., & Ithnin, N. (2016). Factors influencing cloud computing adoption for e-government implementation in developing countries: Instrument development. *Journal of Systems and Information Technology*, *18*(3), 297–327. https://doi.org/10.1108/JSIT-01-2016-0001

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods*, *1*(2), 13–22. https://doi.org/10.1177/160940690200100202

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Musiani, F. (2022). Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. *Information Communication and Society*, *0*(0), 1–16. https://doi.org/10.1080/1369118X.2022.2049850

Nanos, I., Manthou, V., & Androutsou, E. (2019). Cloud Computing Adoption Decision in E-government. *Springer Proceedings in Business and Economics*, 125–145. https://doi.org/10.1007/978-3-319-95666-4_9

Nohrstedt, D., & Olofsson, K. (2016). A Review of Applications of the Advocacy Coalition Framework in Swedish Policy Processes. *European Policy Analysis*, *2*(2). https://doi.org/10.18278/epa.2.2.3

Noyan, O. (2021). EU and US working together on trusted connectivity to counter China. *Euractiv*. https://www.euractiv.com/section/digital/news/eu-and-us-working-together-on-trusted-connectivity-to-counter-china/

Nugraha, Y., Kautsarina, & Sastrosubroto, A. S. (2015). Towards data sovereignty in cyberspace. *2015 3rd International Conference on Information and Communication Technology, ICoICT 2015*, 465–471. https://doi.org/10.1109/ICoICT.2015.7231469

Oertel, J. (2020). Europe's Digital Sovereignty: From rulemaker to superpower in the age of US-China rivalry. *European Council on Foreign Relations*, *1*, 24–31.

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. *Journal of Cloud Computing*, *5*(1). https://doi.org/10.1186/s13677-016-0054-z

Ospina, S. M., Esteve, M., & Lee, S. (2018). Assessing Qualitative Studies in Public Administration Research. *Public Administration Review*, *78*(4), 593–605.

https://doi.org/10.1111/puar.12837

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, *27*(3), 245–253. https://doi.org/10.1016/j.giq.2010.01.002

Parasol, M. (2018). The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams. *Computer Law and Security Review*, *34*(1), 67–98. https://doi.org/10.1016/j.clsr.2017.05.022

Patterson, M. E., & Williams, D. R. (1998). Paradigms and problems: The practice of social science in natural resource management. *Society and Natural Resources*, *11*(3), 279–295. https://doi.org/10.1080/08941929809381080

Pearson, S. (2013). Privacy, Security and Trust in Cloud Computing. In S. Pearson & G. Yee (Eds.), *Privacy and Security for Cloud Computing* (pp. 3–42). Springer. https://doi.org/10.1007/978-1-4471-4189-1_1

Pedreira, V., Barros, D., & Pinto, P. (2021). A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. *SENSORS*, *21*(15). https://doi.org/10.3390/s21155189

Phuthong, T. (2022). Factors that influence cloud adoption in the public sector: The case of an emerging economy—Thailand. *Cogent Business and Management*, *9*(1). https://doi.org/10.1080/23311975.2021.2020202

Pierce, J. J., Giordono, L. S., Peterson, H. L., & Hicks, K. C. (2022). Common approaches for studying advocacy: Review of methods and model practices of the Advocacy Coalition Framework. *Social Science Journal*, *59*(1), 139–158. https://doi.org/10.1016/j.soscij.2019.06.005

Pierce, J. J., Peterson, H. L., & Hicks, K. C. (2020). Policy Change: An Advocacy Coalition Framework Perspective. *Policy Studies Journal*, *48*(1), 64–86. https://doi.org/10.1111/psj.12223

Pigatto, J. T., Datysgeld, M. W., & da Silva, L. G. P. (2021). Internet governance is what global stakeholders make of it: a tripolar approach. *REVISTA BRASILEIRA DE POLITICA INTERNACIONAL*, *64*(2). https://doi.org/10.1590/0034-7329202100211

Pistor, K. (2020). Statehood in the digital age 1 . *Constellations*, *27*(1), 3–18. https://doi.org/10.1111/1467-8675.12475

Pohle, J. (2020). *Digital sovereignty: A new key concept of digital policy in Germany and Europe*.

Pohle, J., & Thiel, T. (2020). Digital Sovereignty. *Internet Policy Review*, *9*(4), 1–19. https://doi.org/10.15211/SOVEUROPE220214049

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy and Internet*, *14*(1), 13–27. https://doi.org/10.1002/poi3.296

Potschka, M. (2018). Peirce' s Concept of Abduction (Hypothesis Formation) across His Later Stages of Scholarly Life. *The Commens Working Papers*, 70. http://www.commens.org/papers/paper/potschka-martin-2018- peirce's-concept-abduction-hypothesis-formation- across-his-later 2342-4532

Prasad, R. (2022). People as data, data as oil: the digital sovereignty of the Indian state. *Information, Communication & Society*. https://doi.org/10.1080/1369118X.2022.2056498

Radaelli, C. M. (1999). Harmful tax competition in the EU: Policy narratives and advocacy coalitions. *Journal of Common Market Studies*, *37*(4), 661–682. https://doi.org/10.1111/1468-5965.00201

Renda, A. (2020). Artificial intelligence: Towards a pan-European strategy. In C. Hobbs (Ed.), *Europe's Digital Sovereignty: From rulemaker to superpower in the age of US-China rivalry* (pp. 54–62). European Council on Foreign Relations.

Renda, A. (2021). Making the digital economy "fit for Europe." *European Law Journal*, *26*(5–6), 345–354. https://doi.org/10.1111/eulj.12388

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet*

Policy Review, *10*(3). https://doi.org/10.14763/2021.3.1575

Robson, C., & McCartan, K. (2016). *Real World Research* (Fourth Edi). Wiley.

Ronquillo, J. G., Winterholler, J. E., Cwikla, K., Szymanski, R., & Levy, C. (2018). Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information. *JAMIA Open*, *1*(1), 15–19. https://doi.org/10.1093/jamiaopen/ooy019

Rosati, P., & Lynn, T. (2020). Measuring the Business Value of Infrastructure Migration to the Cloud. In T. Lynn, J. G. Mooney, P. Rosati, & G. Fox (Eds.), *The Business Value of Cloud Computing* (pp. 19–29). Palgrave Macmillan. http://www.palgrave.com/gp/series/16004

Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. *Minds and Machines*, *31*, 439–456. https://doi.org/10.1007/s11023-021-09566-7

Sabatier, P. (1988). An Advocacy Coalition Framework of Policy Change and the Role of Policy-Oriented Learning Therein. *Policy Sciences*, *21*(2), 129–168.

Sabatier, P. (1998). The advocacy coalition framework: Revisions and relevance for Europe. *Journal of European Public Policy*, *5*(1), 98–130. https://doi.org/10.1080/13501768880000051

Sabatier, P., & Weible, C. (2007). The Advocacy Coalition Framework: Innovations and Clarifications. In P. Sabatier (Ed.), *Theories of the Policy Process* (pp. 189–220). Westview Press.

Saunders, M. A., Lewis, P., & Thornhill, A. (2012). Research Methods for Business Students. In *Research Methods for Business Students* (Sixth edit). Pearson.

Schneider, I. (2020). Democratic governance of digital platforms and artificial intelligence? Exploring governance models of china, the us, the eu and mexico. *EJournal of EDemocracy and Open Government*, *12*(1), 1–24. https://doi.org/10.29379/jedem.v12i1.604

Schniderova, L. (2022). EU strategic autonomy must remain open, says Czech deputy PM. *Euractiv*. https://www.euractiv.com/section/digital/news/eu-strategic-autonomy-must-remain-open-says-czech-deputy-pm/

Scholl, H. J. (2021). The Digital Government Reference Library (DGRL) and its potential formative impact on Digital Government Research (DGR). *Government Information Quarterly*, *38*(4), 101613. https://doi.org/10.1016/j.giq.2021.101613

Scoon, C., & Ko, R. K. L. (2016). The data privacy matrix project: Towards a global alignment of data privacy laws. *Proceedings - 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 10th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Symposium on Parallel and Distributed Proce*, 1998–2005. https://doi.org/10.1109/TrustCom.2016.0305

Shanahan, E. A., Jones, M. D., & McBeth, M. K. (2018). How to conduct a Narrative Policy Framework study. *Social Science Journal*, *55*(3), 332–345. https://doi.org/10.1016/j.soscij.2017.12.002

Shapiro, J. (2020). Europe's Digital Sovereignty: From rulemaker to superpower in the age of US-China rivalry. In C. Hobbs (Ed.), *European Council on Foreign Relations* (pp. 13–23). European Council on Foreign Relations. https://www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf

Sheikh, H. (2022). European Digital Sovereignty: A Layered Approach. *Digital Society*, 1–25. https://doi.org/10.1007/s44206-022-00025-z

Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication*, *9*(3), 304–324. https://doi.org/10.1080/17544750.2016.1206028

Simmons, J. P., Nelson, L. D., & Simonsohn, U. (2011). False-positive psychology: Undisclosed flexibility in data collection and analysis allows presenting anything as significant. *Psychological Science*, *22*(11), 1359–1366. https://doi.org/10.1177/0956797611417632

Smyrl, M. E. (1998). When (and how) do the Commission's preferences matter? *Journal of Common Market Studies*, *36*(1), 79–100. https://doi.org/10.1111/1468-5965.00098

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, *104*(July), 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Swire, P., & Kennedy-Mayo, D. (2022). The Effects of Data Localization on Cybersecurity. *SSRN Electronic Journal*, 1–44. https://doi.org/10.2139/ssrn.4030905

Tan, E., & Crompvoets, J. (2022). A new era of digital governance. In E. Tan & J. Crompvoets (Eds.), *The New Digital Era Governance: How New Digital Technologies Are Shaping Public Governance* (pp. 13–49). Wageningen Academic Publishers. https://doi.org/10.3920/978-90-8686-930-5

Tancock, D., Pearson, S., & Charlesworth, A. (2013). A Privacy Impact Assesment Tool for Cloud Computing. In S. Pearson & G. Yee (Eds.), *Privacy and Security for Cloud Computing*. Springer. https://doi.org/10.1007/978-1-4471-4189-1_3

Taylor, A. R. E. (2021). Future-proof: bunkered data centres and the selling of ultra-secure cloud storage. *Journal of the Royal Anthropological Institute*, *27*, 76–94. https://doi.org/10.1111/1467-9655.13481

Taylor, R. D. (2020). "Data localization": The internet in the balance. *Telecommunications Policy*, *44*(8), 102003. https://doi.org/10.1016/j.telpol.2020.102003

Templier, M., & Paré, G. (2015). A framework for guiding and evaluating literature reviews. *Communications of the Association for Information Systems*, *37*, 112–137. https://doi.org/10.17705/1cais.03706

Thumfart, J. (2020). Public and private just wars: Distributed cyber deterrence based on vitoria and grotius. *Internet Policy Review*, *9*(3), 1–26. https://doi.org/10.14763/2020.3.1500

Thumfart, J. (2021). The COVID-Crisis as Catalyst for the Norm Development of Digital Sovereignty. Building Barriers or Improving Digital Policies? *SSRN Electronic Journal*, 15–16. https://doi.org/10.2139/ssrn.3793530

Timmermans, S., & Tavory, I. (2012). Theory construction in qualitative research: From grounded theory to abductive analysis. *Sociological Theory*, *30*(3), 167–186. https://doi.org/10.1177/0735275112457914

Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines*, *29*(4), 635–645. https://doi.org/10.1007/s11023-019-09508-4

Timmers, P. (2022a). Strategic Autonomy Tech Alliances: Political-Industrial Collaboration in Strategic Technologies. In *Strategic Autonomy Series*. https://doi.org/10.4324/9781003248392-7

Timmers, P. (2022b). The Technological Construction of Sovereignty. *Perspectives on Digital Humanism*, 213–218. https://doi.org/10.1007/978-3-030-86144-5_28

Trakadas, P., Nomikos, N., Michailidis, E. T., Zahariadis, T., Facca, F. M., Breitgand, D., Rizou, S., Masip, X., & Gkonis, P. (2019). Hybrid clouds for data-intensive, 5G-enabled IoT applications: An overview, key issues and relevant architecture. *Sensors (Switzerland)*, *19*(16). https://doi.org/10.3390/s19163591

Turab, N. M., Taleb, A. A., & Masadeh, S. R. (2013). Cloud Computing Challenges And Solutions. *International Journal of Computer Networks & Communications*, *5*(5), 209–216. https://doi.org/10.5121/ijcnc.2013.5515

US Department of State. (2021). *The Clean Network*. https://2017-2021.state.gov/the-clean-network/index.html

US Department of State. (2022). *Blue Dot Network*. https://www.state.gov/blue-dot-network/

van de Hoven, J., Comandè, G., Ruggieri, S., Domingo-Ferrer, J., Musiani, F., Gianotti, F., Pratesi, F., & Stauch, M. (2021). Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications. *Opinio Juris In In Comparatione*, *1*, 131–156.

van Eerd, M. C. J., & Wiering, M. A. (2022). The politics of practical implementation: reloading of information by competing coalitions in EU water governance. *International Journal of Water Resources Development*, *38*(4), 579–595. https://doi.org/10.1080/07900627.2021.1999218

van Thiel, S. (2014). *Research Methods in Public Administration and Public Management*. Routledge.

Wagle, S. S. (2017). *SLA Violation Detection Model and SLA Assured Service Brokering (SLaB) in Multi-Cloud Architecture* [Università di Bologna]. http://amsdottorato.unibo.it/7791/

Walliman, N. (2011). Research Methods: The Basics. In *Research Methods*. Routledge. https://doi.org/10.4324/9781003141693-4

Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii. https://doi.org/10.1.1.104.6570

Weible, C., & Sabatier, P. (2006). *A Guide to the Advocacy Coalition Framework*. *December 2006*, 123–136. https://doi.org/10.1201/9781420017007.pt3

Weible, C., & Sabatier, P. (2009). Coalitions, science, and belief change: Comparing adversarial and collaborative policy subsystems. *Policy Studies Journal*, *37*(2), 195–212. https://doi.org/10.1111/j.1541-0072.2009.00310.x

Weible, C., Sabatier, P., Jenkins-Smith, H. C., Nohrstedt, D., Henry, A. D., & DeLeon, P. (2011). A quarter century of the advocacy coalition framework: An introduction to the special issue. *Policy Studies Journal*, *39*(3), 349–360. https://doi.org/10.1111/j.1541-0072.2011.00412.x

Weible, C., Sabatier, P., & McQueen, K. (2009). Themes and variations: Taking stock of the advocacy coalition framework. *Policy Studies Journal*, *37*(1), 121–140. https://doi.org/10.1111/j.1541-0072.2008.00299.x

Wenhong, X. (2020). Challenges to cyber sovereignty and response measures. *World Economy and International Relations*, *64*(2), 89–99. https://doi.org/10.20542/0131-2227-2020-64-2-89-99

White House. (2022). *A Declaration for the Future of the Internet*. https://www.whitehouse.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet_Launch-Event-Signing-Version_FINAL.pdf

Woon, C. Y. (2021). "Provincialising" the Belt and Road Initiative: Theorising with Chinese narratives of the "Digital Silk Road" (sic). *ASIA PACIFIC VIEWPOINT*, *62*(3), 286–290. https://doi.org/10.1111/apv.12320

Yan, X. (2020). Bipolar rivalry in the early digital age. *Chinese Journal of International Politics*, *13*(3), 313–341. https://doi.org/10.1093/cjip/poaa007

Yilmaz, S. (2018). Advancing our understanding of the EU sports policy: the socio-cultural model of sports regulation and players' agents. *International Journal of Sport Policy*, *10*(2), 353–369. https://doi.org/10.1080/19406940.2018.1432671

Yun, C. (2019). External shocks and policy change in different coalition opportunity structures. *International Review of Public Administration*, *24*(1), 17–35. https://doi.org/10.1080/12294659.2019.1577558

Zarkadakis, G. (2022). The Internet Is Dead: Long Live the Internet. In H. Werthner, E. Prem, E. A. Lee, & C. Ghezzi (Eds.), *Perspectives on Digital Humanism* (pp. 47–52). Springer International Publishing. https://doi.org/10.1007/978-3-030-86144-5_7

Zhao, Y. (2010). China's pursuits of indigenous innovations in information technology developments: Hopes, follies and uncertainties. *Chinese Journal of Communication*, *3*(3), 266–289. https://doi.org/10.1080/17544750.2010.499628

Zrenner, J., Möller, F. O., Jung, C., Eitel, A., & Otto, B. (2019). Usage control architecture options for data sovereignty in business ecosystems. *Journal of Enterprise Information Management*, *32*(3), 477–495. https://doi.org/10.1108/JEIM-03-2018-0058

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuiderwijk, A., Chen, Y. C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, *38*(3), 101577. https://doi.org/10.1016/j.giq.2021.101577

Zwattendorfer, B., Stranacher, K., Tauber, A., & Reichstädter, P. (2013). Cloud computing in e-government across Europe: A comparison. *Lecture Notes in Computer Science*, *8061 LNCS*, 181–195. https://doi.org/10.1007/978-3-642-40160-2_15

Zygmuntowski, J. J., Zoboli, L., & Nemitz, P. F. (2021). Embedding european values in data governance: A case for public data commons. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1572

Appendices

A Anonymized list of interview participants

Participant No.	Organizational affiliation	Reason for inclusion	Interview type
Participant 1	Czech government – Interior Ministry; Prague School of Economics	*Creator of Czech eGovernment cloud; familiarity with MSCCG*	*open*
Participant 2	EC, DG DIGIT	*Familiarity with EC cloud procurement policies*	*open*
Participant 3	EC, DG Joint Research Centre	*Familiarity with EC cloud procurement policies*	*open*
Participant 4	Unnamed EU-headquartered CSP	*Source of initial briefing on the services offered to governments*	*semi-structured*
Participant 5	Czech government – Interior Ministry	*Creator of Czech eGovernment cloud; familiarity with MSCCG; referral by Participant 1*	*semi-structured*
Participant 6	French government – Inter-ministerial Directorate for Digital Affairs	*Familiarity with MSCCG and the French cloud strategy; referral by Participant 8*	*semi-structured*
Participant 7	Czech government – Technology Agency of the Czech Republic	*Familiarity with the cloud procurement policies of the Czech government*	*semi-structured*
Participant 8	EC, DG CNECT	*Familiarity with MSCCG and the EUCS*	*semi-structured*
Participant 9	Unnamed U.S.-headquartered CSP	*Source of initial briefing on the services offered to governments*	*semi-structured*
Participant 10	French tech media company	*Familiarity with the French digital sovereignty debate*	*semi-structured*
Participant 11	Italian government – Digital Transformation Department	*Creator of the Italian Cloud Strategy; familiarity with MSCCG; referral by Participant 6*	*semi-structured*
Participant 12	Czech government – Cabinet of Deputy Prime Minister for Digitalization	*Source of insight into the foreign policy dimension of digital sovereignty*	*semi-structured*
Participant 13	French government – Interior Ministry	*Source of insight into the French government experience with cloud*	*semi-structured*

B Interview manual

(1) Introduction

- Which organization do you work for and what is your role?
- What is your experience with public sector migration to the cloud or national cloud strategy development?
- How do you understand the terms “digital sovereignty” and “European digital sovereignty?”

(2) The national context

- How is cloud adoption progressing in the <*country*> public sector?
- What are the main pillars of <*your country’s*> national cloud strategy?
- What is <*your country’s*> assessment of the main threats to its digital sovereignty? How did this position come about? Do different communities/groups within <*your country*> have different perceptions?
- I would particularly appreciate your reflection on the threat posed by contracting non-EU hyperscalers (incl. their EU-based subsidiaries). In your personal view (or in your organization’s view), do the CLOUD Act and FISA pose a real risk to EU citizens’ data sovereignty? If so, in which ways (and how effectively) is this risk offset by different national and EU level measures?

(3) The EU context

- What are the dynamics of the Member State working group of the European Alliance for Industrial Data, Edge and Cloud? *(if applicable)*
- Are there any cleavages or tensions? Which aspects of national government cloud strategies are most difficult to harmonize?
- Are efforts to achieve EU-level and national-level digital sovereignty ever at odds?
- Are countries such as France and Germany ever accused of using the digital sovereignty/strategic autonomy rhetoric as a tactic to promote their own companies at the expense of others?

C List of primary sources used in document analysis

Document No.	Title	Referred By
Document 1	Alliance for Industrial Data, Edge and Cloud – WG MSCCG – Agenda and Minutes	*Participant 1*
Document 2	Drawing up a panorama of national cloud policies in the EU (presentation by the French Presidency)	*Participant 7*
Document 3	Study to support an Impact Assessment on enhancing the use of data in Europe	*Participant 8*
Document 4	European Commission Cloud Strategy	*Participant 2*
Document 5	French National Cloud Strategy	*Participant 13*
Document 6	Czech National Cloud Strategy	*Participant 5*
Document 7	Italian Cloud Strategy	*Participant 11*
Document 8	Council Conclusions on the New European Innovation Agenda	*Participant 12*

D ACF-based coding frame

ACF concept	Code name	Operational definition of code
Policy subsystem	Policy subsystem description	Respondent characterizes a policy subsystem in which cloud computing is discussed
Coalition	Coalition structure – EU-level	Respondent mentions any alliances or cleavages within the policy subsystem at the EU-level
	Coalition structure – national or organizational level	Respondent mentions any alliances or cleavages within the policy subsystem at the national or organizational level
	Coalition resources	Respondent refers to the policy-relevant resources leveraged by a coalition
	Coalition coordination	Respondent reveals a way in which a coalition engages in coordination
	Policy-specific behavior	Respondent refers to an example of policy-specific behavior (by a coalition)
Deep core belief	Deep core belief – policy actor	Respondent directly or indirectly expresses their deep core belief or refers to the deep core belief of another policy actor
	Deep core belief – coalition	Respondent alludes to the deep core belief shared across a coalition
Policy core belief	Policy core belief – policy actor	Respondent refers to their own or another policy actor's policy core belief
	Policy core belief – coalition	Respondent refers to a policy core belief around which a coalition has formed
Secondary belief	Secondary belief – policy actor	Respondent expresses a judgment regarding the practical details of (cloud-related) policy implementation, or mentions another actor's opinion on the secondary aspects of policy
	Secondary belief – coalition	Respondent refers to the secondary beliefs shared across a coalition
Policy broker	Policy broker	Respondent refers to the EU-level policy broker
Governmental authority	Governmental authority	Respondent refers to an EU or national-level governmental authority that makes policy decisions and oversees the policymaking infrastructure
Policy output	Policy output – national	Respondent refers to a policy output (which may be already in place or still in preparation) at the national level
	Policy output – EU	Respondent refers to a policy output at the EU level
Policy impact	Policy impact – national	Respondent refers to some form of impact of a national-level policy
	Policy impact – EU	Respondent refers to some form of impact of an EU-level policy
Relatively stable parameters	Stable parameters	Respondent mentions one of the four possible relatively stable parameters within which the policy subsystem operates (basic attributes of the problem area; basic distribution of natural resources; values and structure of the society; basic constitutional structure)
Long-term coalition opportunity structures	Long-term coalition opportunities	Respondent mentions one of the possible features of the coalition opportunity structure (societal conflict; the amount of consensus needed for policy change; the degree of openness of the political system)

ACF concept	Code name	Operational definition of code
Short-term constrains of policy actors	Short-term coalition constraints	Respondent refers to the short-term effects of external system events or long-term coalition opportunity structures, on a coalition
External event	External shock	Respondent describes the way in which an external event (such as technological or socioeconomic change; public opinion change following a disaster or crisis; government change; or policy change in other policy subsystems) brings public attention to the policy problem
	External event leading to internal shock	Respondent describes the way in which an external event destabilizes internal subsystem practices
Policy-oriented learning	Learning about policy	Respondent describes an instance of information transfer across policy actors or coalitions, related to cloud policy at the strategic level
	Learning about technical aspects	Respondent describes an instance of information transfer across policy actors or coalitions, related to cloud policy at the technical level
Policy change	Policy change – EU	Respondent mentions a change in an EU-level policy and/or its causes
	Policy change – national	Respondent mentions a change in a national-level policy and/or its causes
Venue	Venue	Respondent refers to a specific institutional context in which policy deliberation takes place and/or where policy decisions can be made
Negotiated agreement	Negotiated agreement	Respondent refers to a policy compromise reached by opposing coalitions, or to an attempt at reaching one

Source: the author, primarily based on Sabatier (1988)

Note: the above coding frame was applied to both interview data and the documents listed in Appendix C. In the case of the latter, the word “respondent” in the operational definitions of the codes was replaced with “document section.”

E ACF-based codebook

This Codebook depicts the number of instances each code was found in the interview transcripts and in the analyzed documents. “Files” refers to the number of individual files (i.e. interview transcripts or documents) in which the code appeared, whereas “Ref.” is short for the overall number of occurrences across all files.

Code Name	Files – Int.	Ref. – Int.	Files – Doc.	Ref. – Doc.
Policy subsystem description	12	33	7	24
Coalition structure – EU-level	7	20	2	16
Coalition structure – national or organizational level	4	12	0	0
Coalition resources	2	8	2	6
Coalition coordination	10	35	2	66
Policy-specific behavior	2	4	0	0
Deep core belief – policy actor	3	8	4	35
Deep core belief – coalition	2	5	0	0
Policy core belief – policy actor	12	67	4	21
Policy core belief – coalition	12	81	0	0
Secondary belief – policy actor	12	36	2	5
Secondary belief – coalition	12	43	1	5
Policy broker	7	20	0	0
Governmental authority	5	45	7	36
Policy output – national	11	67	7	82
Policy output – EU	10	82	7	45
Policy impact – national	7	9	4	14
Policy impact – EU	5	23	2	6
Stable parameters	3	5	1	1
Long-term coalition opportunities	4	6	1	6
Short-term coalition constraints	2	3	1	1
External shock	3	6	1	1
External event leading to internal shock	4	7	0	0
Learning about policy	5	11	0	0
Learning about technical aspects	7	56	3	6
Policy change – EU	9	25	7	24
Policy change – national	7	34	7	45
Venue	12	59	7	16
Negotiated agreement	4	11	1	4

F Examples of code applications – ACF-based coding frame

Code name	Example	Source
External shock	"There have been many cases. Regio de Lazio was hacked by a group trying to steal data and get their money. Also in Torino, schools got hacked. Recently, the last one in Torino was hospitals. And because the public administrations are going to be responsible for that, they want to have the best solution to deal with that situation. We are explaining to them that ransomware is attacking their infrastructure. There are few ransomware cases in the cloud!"	*Participant 11*
Learning about technical aspects	"The second problem is that you can't technically, at least not in any way that is affordable, deploy such offsite decryption key storage, for SaaS solutions. Or for any solutions that imply data in transit."	*Unnamed participant*
Coalition structure – EU level	"Then there is what we call the business community – they are not IT specialists but users of IT tools for the objectives of their policies – there, we see more of a lack of knowledge. Sometimes they are responsible for a website and they don't even know if the website is hosted on the cloud or not. Also they have a negative perception regarding security (an impression that the data will be lost if in cloud). You can tell them it is very safe (the IT community thinks so) but they can't be sure. There is a political dimension."	*Participant 2*
Learning about policy	"What we have in common: • Cloud First (meaning Public Cloud First)! • Cloud adoption is a key lever for Public Action modernization • The crucial role played by the General Data Protection Regulation and Cybersecurity labels in building Trusted Cloud Services • We represent a great opportunity for European Key Players • A lot to learn (and share) from each other"	*Document 2*

G Recent innovations in cloud

Below is a passage that is not pertinent enough to the core subject of this thesis to be included in the literature review chapter, but nevertheless provides useful background information for readers who are interested.

Any account on cloud computing would be incomplete without covering recent innovations in the field, many of which do not fit in the above classification frameworks. Lynn et al. (2020) discuss several developments that have been changing the "nature of the cloud" (p. 109). The first one is *containerization*, whereby all components necessary to run a specific program – the software code and all its dependencies such as libraries – are packaged together in discrete "containers" that are less resource-intensive and more portable than entire virtual machines, thus reducing opportunities for lock-in (Lynn et al., 2020). Another innovation is *serverless cloud computing*, a software architecture where an application is decomposed into events and "stateless" functions hosted on a platform where they can be executed on-demand via an application programming interface (API). This service model is referred to as Function as a Service (FaaS), where the customer is only charged for the resources consumed during the execution of the function (Lynn et al., 2020; Trakadas et al., 2019). Other recent developments include the *heterogeneous cloud*, which is an architecture that includes both general purpose processors and hardware with specialized processing capabilities that can accommodate Big Data analytics or high-performance computing (Lynn et al., 2020). Similarly, the *composable cloud* decouples resources (e.g., memory or storage) from the hardware on which they reside, inserting a control software layer that can reallocate resources according to the requirements of a given set of workloads, thus dramatically reducing the prevalence of overprovisioning (Lynn et al., 2020). In heterogeneous and composable clouds, particularly when applied on a large scale, the complexity of configurations and component interactions is too high to be managed manually. Thus, CSPs often deploy another innovation – *AIOps* (AI for IT Operations), where machine learning and artificial intelligence are used to optimally manage capacity planning, resource and storage utilization, and threat detection and analysis in distributed systems (Masood & Hashmi, 2019).

New computing paradigms stemming from cloud computing also form the backbone of the *Internet of Things* (IoT), which can be defined as an information network through which physical objects (i.e., devices ranging from sensors to smartphones) actively interact and collaborate with each other (Andreas et al., 2021; Lynn et al., 2020). Computing resources are distributed across the IoT in a decentralized manner, where data processing takes place not only in the cloud, but also at the level of the device (*edge computing*) or a layer of nodes in between the cloud and the devices (*fog computing* and *mist computing*) (Biswash & Jayakody, 2020; Lynn et al., 2020).

H Organizational drivers of and barriers to cloud adoption

Below is a passage that is not pertinent enough to the core subject of this thesis to be included in the literature review chapter, but nevertheless provides useful background information for readers who are interested.

Organizational drivers. Complementing the technological, budgetary, legal, and security considerations discussed above, the empirical literature on government adoption of cloud computing technology provides crucial insight into the social and organizational dynamics behind cloud adoption and non-adoption outcomes. Articles studying these dynamics, which often apply various task-technology fit and technology acceptance models (Buavirat et al., 2019; Liang et al., 2017), find that the key drivers of cloud computing adoption include the anticipated benefit, especially the perceived quality and ease of use of cloud system features; this includes reliability, flexibility, and responsiveness, which (are expected to) lead to business process optimization and/or standardization (Ali et al., 2021; Johansson & Ruivo, 2013; Liang et al., 2017; Phuthong, 2022). According to Johansson and Ruivo (2013), customers' enthusiasm for SaaS solutions is mostly driven by the fact that the risk of a potentially poor implementation shifts from the customer to the supplier. Some government employees also advocate for SaaS systems because they make remote work possible (Jones et al., 2019). Other researchers find that a positive image of specific CSPs also drives adoption, e.g., due to initial trust in the supplier given their strong market position and reputation (Liang et al., 2017), or following a prior relationship where the supplier made the customer feel valued through individual attention and support (Liang et al., 2017; Phuthong, 2022). Additional key organizational drivers of cloud adoption include the availability of best practice examples from other public sector organizations to learn from, competitive pressure between agencies to deliver on the central government's digital transformation commitments, and organizational readiness, which increases with a culture of innovativeness, employee autonomy, the existence of cloud project champions, and top management support (Abied et al., 2022; Ali et al., 2021; Johansson & Ruivo, 2013; Jones et al., 2019; Liang et al., 2017).

Organizational barriers. The main individual-level factors that may inhibit cloud adoption in the public sector include a lack of awareness about or confidence in the benefits of cloud computing applications among top management (Nanos et al., 2019; Paquette et al., 2010); individual employees' fear of loss in IT control (Nanos et al., 2019) and data sovereignty (Liang et al., 2017; Paquette et al., 2010); concerns about the appropriateness of outsourcing the management of government documents to (foreign) private entities (Paquette et al., 2010); and general resistance to change or unwillingness to expend the effort necessary to learn to work with new systems (which can be exacerbated by regular experience of work overload) (Abied et al., 2022; El-Gazzar et al., 2016; Nanos et al., 2019). Among the organizational-level barriers to cloud computing diffusion in the public sector are organizational inertia and rigidity of IT-related processes (Liang et al., 2017); the complexity or perceived degree of professional risk

involved in the process of selecting the appropriate cloud solution and vendor (Liang et al., 2017; Nanos et al., 2019); and lack of understanding of the correct way of applying the relevant institutional and regulatory frameworks to the (novel) context of cloud computing services (coupled with a fear of the consequences of misinterpretation) (El-Gazzar et al., 2016; Liang et al., 2017; Nanos et al., 2019). In addition, training staff to use – or hiring new staff to implement – cloud technology might be perceived as too time-consuming or difficult (El-Gazzar et al., 2016). Notably, organization size plays a role – smaller, especially local-level public sector organizations tend to adopt cloud computing technology at a slower rate than for example ministries (Ali et al., 2021). Smaller organizations may lack IT expertise or the power to challenge the standard SLA terms offered by large CSPs. They might also be afraid of the possibility of vendor lock-in by a cloud supplier (alternatively, they may already be locked-in by a non-cloud vendor and therefore be unable to consider switching to a particular cloud service). (Abied et al., 2022; Ali et al., 2021; El-Gazzar et al., 2016) The institutional policy-related obstacles to cloud adoption in public sector organizations include a delayed deployment of national data protection or data ownership legislation (Paquette et al., 2010) or of a national e-government, data, or government cloud computing strategy; or these strategies might not yet be accompanied by clear performance metrics for government organizations (Liang et al., 2017; Nanos et al., 2019). Public servants in some countries also hesitate to take action due to the discontinuity of adopted policies at every government change (Nanos et al., 2019). Finally, traditional public procurement procedures are often incompatible with the context of cloud-based services (especially SaaS products) (Irion, 2012; McGillivray, 2022).

I Evolution of research question

It should be acknowledged that the research question and objectives have evolved throughout the drafting process. The initial title of the thesis – "Government Cloud Computing in the EU: Reconciling Market Realities and Bilateral Partnerships with Digital Sovereignty Commitments" – was modified in light of new information. Specifically, the author's initial assumption was that international negotiation frameworks and partnerships such as the TTC would be relevant to the discussion. However, Participant 8 corrected this view, and so this assumption was discarded. Simultaneously, it only emerged throughout the interviewing process that something akin to coalitions is forming in the debate – only then was it decided to use the ACF methodology and incorporate a referenced to coalitions in the research question.

J Literature review protocol

Aim (I): to define and contextualize key terms and concepts related to "European digital sovereignty"			
Search String (SS); No. of "Work Queue" items per database (incl. duplicates)	Web of Science	Scopus	DGRL
SS1: TITLE-ABS-KEY ("digital sovereignty" OR "data sovereignty" OR "network sovereignty" OR "cyber sovereignty" OR "technological sovereignty" AND NOT "indigenous") AND (LIMIT-TO (LANGUAGE , "English"))	290 results	327 results	N/A
Inclusion criteria for SS1: (a) article likely to contain a definition of one of the five terms; or (b) article likely to discuss a closely related concept, important to understand the context of one of the five terms			
SS1: No. of (unique) articles passing inclusion criteria (keyword (KW) + backward (BW) & forward (FW) searches)	Approx. 100 (80 KW + 10 BW + 10 FW)		
Aim (II): to define and contextualize key terms and concepts related to "government cloud computing"			
SS; No. of "Work Queue" items per database (incl. duplicates)	Web of Science	Scopus	DGRL
SS2: TITLE-ABS-KEY ("cloud" AND "government" OR "public sector") AND (LIMIT-TO (LANGUAGE , "English"))	Approx. 500	Approx. 500	Approx. 20
Inclusion criteria for SS2: (a) article gives a basic overview of the most important aspects of cloud computing (this was mostly relevant for backward searches); or (b) article discusses the issues of government cloud computing adoption, either from an organizational or from a legal perspective; and (c) article is cited at least 10 times (to initially narrow down the large number of results)			
SS2: No. of (unique) articles passing inclusion criteria (KW + BW & FW searches)	Approx. 50 (40 KW + 10 BW + 0 FW)		
Aim (III): to review material that can aid in understanding and correctly applying the conceptual framework (the advocacy coalition framework)			
SS; No. of "Work Queue" items per database (incl. duplicates)	Web of Science	Scopus	DGRL
SS3: TITLE-ABS-KEY ("Advocacy Coalition Framework" OR "ACF") AND (LIMIT-TO (LANGUAGE , "English"))	Approx. 200	Approx. 200	Approx. 50
Inclusion criteria for SS3: (a) article was written by the framework's proponents; or (b) review article discussing trends in ACF applications; or (c) ACF application related to the EU context			
SS3: No. of (unique) articles passing inclusion criteria (KW + BW & FW searches)	Approx. 30 (20 KW + 5 BW + 5 FW)		

K Measures taken to minimize threats to the reliability, replicability, and internal and external validity of the procedures and results

Area	Relevant threat	Measure(s) taken to counter the threat
Reliability	Participant error	Interviews were conducted at participants' preferred time and using their preferred medium to minimize factors (such as tiredness or being in a rush) that might adversely affect their performance (e.g., the accuracy of their statements or the completeness of the information provided).
	Participant bias	The identity of interviewees is not disclosed to minimize the risk of social desirability bias and other causes of deliberately false responses.
	Researcher error	The likelihood of errors on the part of the researcher was reduced via thorough preparation before interviews, recording as many interviews as possible (so transcripts are available for future scrutiny), and data triangulation in the data analysis stage. A French native speaker was consulted in cases where the researcher's imperfect mastery of the language threatened to be a cause of potential misinterpretations.
	Researcher bias	As a Czech citizen (and an emigrant) and a strong believer in the European project, the author of this study might be reasonably suspected to be (either positively or negatively) biased when collecting and analyzing data related to the Czech and EU case sub-units. However, after some introspection, the author concluded that her desire to learn to produce methodologically rigorous research is much stronger than her motivation to portray any case sub-unit in any particular way to the readers of this thesis. Therefore, the researcher believes it is fair to say that she does not have a preference for any specific research outcome and is thus relatively free of conscious or unconscious researcher bias. Further, effort was made to avoid data collection bias by asking questions in a neutral way, so interviewees do not feel nudged towards confirming the researcher's interim conclusions.
Replica-bility	Researcher degrees of freedom	With the main source of data in this thesis being interviews, it is difficult to imagine the possibility to replicate the results unless the same set of respondents be approached, which is, however, prevented by their anonymization in this thesis. Nevertheless, this study espouses the assumption that only a limited number of viewpoints exist on the topics discussed in this thesis, and the maximum variation sampling technique ensures that the whole range is represented. Thus, a different sample of case sub-units and participants in future studies can be expected to produce similar results if the same sampling technique is followed.
	Improperly reported methodology	Although the author is aware of the replication crisis in the social sciences and acknowledges the impossibility of perfectly documenting and disclosing every step of the research process, effort was made to write a detailed description of the research design and methodology and be fully transparent about the interview guide and coding frames used.
Internal validity	Instrumentation	Not all interviews were audio/video recorded. To mitigate the impact of this inconsistency, the simultaneous notes taken during unrecorded interviews aimed to preserve the exact wording of key statements, which often even led to asking the interviewee to repeat themselves.
	Flawed data extraction	Government elites were interviewed, who can provide optimal quality data; triangulation increased the researcher's understanding of the data.
	Maturation	By choosing a cross-sectional time horizon and being clear about the period in which the data was collected, changes in participants' attitudes that occurred after the interviews, are rendered inconsequential.
External validity	Selection and setting	By virtue of the research question, most of the findings of this study are indeed specific to the case studied. However, using as widely applied a framework as the ACF makes cross-case comparisons of specific aspects of the research topic possible and easy.

Source: the author (based on Bryman, 2012; Epskamp, 2019, p. 151; Leung, 2015; Morse et al., 2002; Robson & McCartan, 2016, pp. 106–108; 112; 369; Saunders et al., 2012, pp. 192–193; and Simmons et al., 2011)

Declaration of Authorship

I hereby declare that, to the best of my knowledge and belief, this Master Thesis titled "The European Digital Sovereignty Debate in the Context of Government Cloud Computing: Policies and Coalitions" is my own work. I confirm that each significant contribution to and quotation in this thesis that originates from the work or works of others is indicated by proper use of citation and references.

Erlangen, 08 December 2022

Michaela Vebrova

Consent Form

for the use of plagiarism detection software to check my thesis

Surname: Vebrova
Given Name: Michaela
Student number: 519164
Course of Study: Public Sector Innovation and eGovernance
Address: Lohweg 16, 92369 Sengenthal, Germany
Title of the thesis: The European Digital Sovereignty Debate in the Context of Government Cloud Computing: Policies and Coalitions

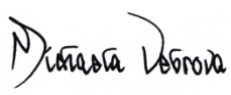
What is plagiarism? Plagiarism is defined as submitting someone else's work or ideas as your own without a complete indication of the source. It is hereby irrelevant whether the work of others is copied word by word without acknowledgment of the source, text structures (e.g. line of argumentation or outline) are borrowed or texts are translated from a foreign language.

Use of plagiarism detection software. The examination office uses plagiarism software to check each submitted bachelor and master thesis for plagiarism. For that purpose the thesis is electronically forwarded to a software service provider where the software checks for potential matches between the submitted work and work from other sources. For future comparisons with other theses, your thesis will be permanently stored in a database. Only the School of Business and Economics of the University of Münster is allowed to access your stored thesis. The student agrees that his or her thesis may be stored and reproduced only for the purpose of plagiarism assessment. The first examiner of the thesis will be advised on the outcome of the plagiarism assessment.

Sanctions. Each case of plagiarism constitutes an attempt to deceive in terms of the examination regulations and will lead to the thesis being graded as "failed". This will be communicated to the examination office where your case will be documented. In the event of a serious case of deception the examinee can be generally excluded from any further examination. This can lead to the exmatriculation of the student. Even after completion of the examination procedure and graduation from university, plagiarism can result in a withdrawal of the awarded academic degree.

I confirm that I have read and understood the information in this document. I agree to the outlined procedure for plagiarism assessment and potential sanctioning.

Erlangen, 08 December 2022



Michaela Vebrova