LUISS

MSc in Law, Digital Innovation and Sustainability

Chair of Data Protection Law

# Data Embassies: A Key to the Puzzle of Data Jurisdiction?


Prof. Filiberto E. Brozzetti

**SUPERVISOR**

Prof. Sofia Ranchordàs

**CO-SUPERVISOR**

Tufarelli Luca

**CANDIDATE**

Identification number: 631733


Academic Year 2024/2025

# *Table of contents*

# Introduction

In the current geopolitical and technological landscape, data has emerged not only as an economic asset but also as a strategic pilar of digital statehood. Essential digital infrastructures such as satellites, cloud systems, and undersea cables now serve not merely technical purposes but are increasingly seen as national extensions of state power. As states more and more rely on globalized digital infrastructure to perform critical functions ranging from public administration to military communications, the question of how to retain authority over data flows has evolved from a technical dilemma to a constitutional and diplomatic imperative.

This thesis arises from the complex and evolving interplay between digital sovereignty, international law and the material infrastructures of cloud and satellite technologies. Specifically, it focuses on the growing phenomenon of data embassies, legal and infrastructural constructs through which states seek to exercise jurisdictional control over their critical data hosted abroad. While the term may (rightfully) evoke metaphors of diplomacy, its true importance is deeply legal and operational: data embassies offer a potential paradigm shift in how sovereignty is projected into cyberspace. They challenge conventional concepts of territorial jurisdiction, open new questions regarding extraterritorial enforcement and emphasize the conflicts between global interconnection and national control.

The Italian government's reported willingness to entrust its governmental communication systems to a private non-EU actor, albeit with the promise of legal safeguards, marks a critical juncture in determining whether existing laws can protect Italy's strategic interests in the digital era. Recent developments, such as the Disegno di Legge Spazio (DDL Spazio), provide a unique lens through which to examine how national governing bodies are attempting to reclaim digital sovereignty, while navigating the risks of technological dependency.

Moreover, this study comes at a time when the conventional pillars of international cooperation are facing significant strain. Multipolar instability, ideological fragmentation and reborn techno-nationalism have become key elements within the global order

post-2025. The United States, under the second Trump administration, has embarked on extensive deregulatory moves and has hardened its stance on export controls, data transfers and strategic technologies. Meanwhile, despite attempts to prove normative leadership through instruments such as the GDPR and the NIS2 directive, the European Union is facing internal fragmentation and declining alignment with allied countries. In this context, Italy's decisions on space and cloud infrastructure could either strengthen its commitment to European digital sovereignty or bring in a new paradigm of strategic alignment, fostered by private non-EU technology providers.

Thus, this thesis not only revolves around data storage or cloud migration policies, but it investigates the transformative impact of data infrastructure over state sovereignty, legal order, and geopolitical alignment. It seeks to determine whether instruments such as the DDL Spazio can provide a viable framework for protecting national interests in a borderless digital environment, as well as whether concepts such as data embassies or trusted orbital zones can provide the operational and legal guarantees required to ensure sovereignty, in an age where the physical location of data is both legally significant and technically obscure.

By combining legal analysis, policy interpretation and technical contextualization, this study aims to provide valuable insights and policies recommendations for legal scholars, policymakers and international law experts. It encourages readers to consider how law must adapt to govern infrastructure that defies territorial logic, as well as how sovereignty may need to be redefined in order to survive the twenty-first century.

## Methodology, Limitations and Scope

This thesis adopts an interdisciplinary multi-layered methodology combining doctrinal legal analysis with geopolitical context assessment and regulatory policy evaluation. The main topic of the study, namely the legal structure of data embassies and their implementation in cross-border data sovereignty as well as satellite communications, needs a comprehensive framework that integrates legal analysis with technological and political aspects. The chosen methodology reflects this complexity, weaving together legal texts, international treaties, comparative legislation and geopolitical developments to provide a holistic and grounded analysis. At its core, the thesis relies on doctrinal le-

gal research, drawing from international law, such as the Vienna Convention on Diplomatic Relations, European Union law, notably the GDPR and national legal frameworks, including the Estonian–Luxembourg data embassy agreement, Bahrain's Cloud Law, and Italy's DDL Spazio. These sources are analysed not in the abstract but in relation to how they interact with emerging infrastructural models such as satellite internet constellations and transnational cloud services.

The analysis is anchored in case studies that reflect the operational and legal divergences of existing models: Estonia's treaty-based data embassy in Luxembourg, Bahrain's private-sector data jurisdiction model and Saudi Arabia's Global AI Hub Law. These case studies are evaluated through close reading of the underlying legal texts, supplemented by academic literature, institutional reports, and primary legislative documents, such as public consultation drafts and explanatory notes. Particular emphasis is placed on understanding the transferability of legal protections in these frameworks and whether they enable functional sovereignty in extraterritorial digital infrastructure.

The Italian case study, especially the alleged Italy-Starlink agreement and the DDL Spazio, is analysed through an in-depth reading of the legislative draft and policy statements by Italian institutions such as AGID and ACN. The analysis draws on both the legal substance of the DDL Spazio, such as its provisions on licensing, strategic infrastructure, and public-private partnerships, and its broader policy implications, including its potential to support data embassy-like mechanisms. The approach integrates primary legislative material with policy commentary to contextualize the law's national and EU implications. Additionally, the research incorporates geopolitical analysis, particularly in relation to the shifting international regulatory and political global environment especially in the EU–U.S. increasing tensions and divergence in various fields such as data protection law and trade dynamics. These developments are treated as dynamic forces that shape the feasibility and strategic desirability of relying on foreign infrastructure, especially in critical areas such as military communications. This aspect of the methodology draws on political analysis, journalistic reporting, and strategic intelligence reports.

Given the limited transparency of private agreements like the alleged Italy–Starlink deal, the thesis does not attempt to verify the terms of the arrangement directly. Instead, it explores the structural and legal risks associated with such arrangements by analysing

the institutional role of actors like SpaceX, especially in light of its current leadership and geopolitical positioning. The methodology here focuses on hypothetical modelling based on publicly known legal precedents and risk evaluation frameworks.

Where possible, technical aspects of satellite internet systems and data center jurisdictions are considered, though not at the engineering level. Instead, industry reports, public documentation, and government regulatory filings are used to capture infrastructure characteristics that have legal implications like data routing opacity, redundancy models or control over network access.

Finally, the methodology remains attentive to comparative legal analysis. Drawing on parallels between Italy's legal instruments and other international best practices, particularly the French Space Operations Act and EU cybersecurity strategy, the research evaluates whether Italy's domestic legal framework is adequate to govern international satellite-based infrastructure. This comparative perspective is used to propose reforms or clarifications, especially around jurisdictional gaps and sovereignty clauses.

This thesis is primarily grounded in the analysis of publicly available legal texts, institutional reports, and secondary literature. As such, it does not rely on confidential agreements, classified government communications, or proprietary technical documentation, particularly in the case of the rumoured agreement between the Italian government and SpaceX. This necessarily limits the analysis to a normative and structural level, rather than an empirical examination of contract enforcement or technical implementation. Hence, the research remains focused on legal feasibility, regulatory coherence, and sovereignty implications, using illustrative examples and comparative cases to ground its arguments. These constraints are acknowledged in order to maintain transparency and to delineate the research within its appropriate doctrinal and policy-oriented scope.

# I. What Are Data Embassies

## I.I Definition and Concept of Data Embassies

In an era where data is one of the most valuable national assets, ensuring its security, sovereignty, and resilience has become a top priority for governments worldwide. Digital infrastructure underpins critical state functions, including public administration, finance, defense, and healthcare. However, nations face increasing threats from cyberattacks, geopolitical tensions, and legal uncertainties surrounding cross-border data storage. This raises a fundamental question: if data is as essential as physical territory, why don't all nations ensure full sovereignty over their digital assets?

Imagine a sovereign nation that urgently needs to store a secure backup of its most sensitive data government records, citizen registries, financial systems, and classified intelligence. This data must remain accessible and intact even in the face of cyber or traditional warfare, natural disasters, or political crises. Under the current global infrastructure, the most widely used solutions are domestic data centers or cloud storage services provided by private companies. Data centers are the backbone of digital infrastructure, enabling the storage, processing, and management of vast amounts of information. However, not all countries have the capability to build and maintain their own data centers, in fact only a handful of nations such as the United States, China, and a few European states possess the necessary resources, technology, and capital to develop self-sufficient digital infrastructure. The vast majority of countries must outsource their data storage to global cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. While these cloud services offer scalability and efficiency, they also introduce significant legal and sovereignty risks. The most pressing concern is data sovereignty, the principle that data is subject to the laws of the country in which it is stored. Governments that rely on foreign-based data centers risk losing control over their most sensitive information, as their data becomes subject to host-

country regulations and external legal frameworks. A key example of this issue is the conflict between the EU's General Data Protection Regulation (GDPR) and U.S. data access laws.[1] A European company storing data in the United States must comply with both EU privacy laws and American government requests for data access, which often conflict, creating legal uncertainty. This problem extends beyond the U.S. and the EU as many governments impose extraterritorial laws that grant them access to data stored beyond their borders.

One of the most controversial examples is the U.S. CLOUD Act (2018)[2], which allows American authorities to compel U.S.-based companies to hand over data, even if it is stored in foreign jurisdictions. This means that companies such as Microsoft, Amazon, and Google, which operate data centers worldwide, be legally required to disclose European or Asian customer data to U.S. law enforcement, even if doing so violates local privacy laws. Similarly, China's Cybersecurity Law (2017)[3] and Russia's Data Localization Law (2015)[4] mandate that foreign companies store data within their respective territories, giving their governments easier access to sensitive information. In some cases, governments have seized or blocked access to data centers operated by foreign companies, citing national security concerns. For example, India's ban on Chinese apps in 2020 resulted in TikTok and WeChat losing access to their Indian data infrastructure.[5] Similarly, Western governments have imposed restrictions on Huawei's data center operations, fearing potential ties to the Chinese government.[6] These actions reflect a growing trend of digital nationalism, where countries seek to control their own digital infrastructure and limit foreign influence over their data systems.

---

[1] European Union. (2016). General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679. Official Journal of the European Union. Available at: https://gdpr.eu/ [Accessed 3 Mar. 2025].

[2] U.S. Congress. (2018). Clarifying Lawful Overseas Use of Data (CLOUD) Act. Available at: https://www.congress.gov/bill/115th-congress/house-bill/4943 [Accessed 3 Mar. 2025].

[3] National People's Congress of China. (2017). Cybersecurity Law of the People's Republic of China. Available at: https://www.chinalawtranslate.com/en/cybersecurity-law-2016/ [Accessed 3 Mar. 2025].

[4] Russian Federation. (2015). Federal Law on Personal Data and Data Localization Requirements. Available at: https://iapp.org/news/a/russias-data-localization-law-requirements-and-compliance/ [Accessed 3 Mar. 2025].

[5] BBC News. (2020). India bans nearly 60 Chinese apps, including TikTok and WeChat, citing security concerns. Available at: https://www.bbc.com/news/world-asia-india-53226295 [Accessed 25 Feb. 2025].

[6] Reuters. (2023). Huawei banned: Which countries have restricted the use of 5G kit? Available at: https://www.reuters.com/world/huawei-banned-which-countries-have-restricted-use-5g-kit-2023-08-10/. [Accessed 3 Mar. 2025].

Additionally, the Schrems II ruling (2020) by the Court of Justice of the European Union (CJEU) further complicated cross-border data transfers[7] by invalidating the EU-U.S. Privacy Shield, citing concerns over U.S. government surveillance practices, and reinforced the principle that European data must remain protected under EU laws, regardless of where it is stored. This has created legal uncertainty for global tech companies, cloud providers, and multinational businesses, forcing them to rethink where and how they store data to avoid potential fines of up to €20 million or 4% of their global revenue.

Recognizing the risks of foreign dependency on cloud storage, European nations have taken steps to develop their own sovereign digital infrastructure. One of the most ambitious projects in this regard is GAIA-X, a European initiative launched in 2020 to create a federated, secure, and transparent cloud ecosystem to reduce European reliance on U.S. and Chinese cloud providers by establishing a framework where data is stored and processed in accordance with EU privacy laws, such as the GDPR.[8] Unlike traditional cloud services, where data is concentrated in a few tech giants' infrastructures, GAIA-X promotes a decentralized network of interoperable cloud providers, ensuring that no single entity has monopolistic control over European data. As Catanzariti aptly defined, "digital sovereignty denotes a form of control over digital assets, which can be material and immaterial entities, thus potentially 'located' in a space that transcends physical boundaries" (Catanzariti, 2024). Although GAIA-X represents an important step towards this concept and provides a more transparent and regulated cloud environment, it does not eliminate the need for physical backup solutions in foreign jurisdictions.

If a government seeks to retain full control over its citizens' data while avoiding the risks associated with third-party providers, what alternative solutions exist? This is where data embassies emerge as a pioneering and highly secure solution.

A Data Embassy is a (usually) government-controlled data center located in a foreign country but operating under the exclusive jurisdiction of the home nation, it serves as a secure offshore backup, ensuring that critical digital services remain functional even in

[7] Court of Justice of the European Union. (2020). Case C-311/18: Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems (Schrems II). Available at: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN. [Accessed 3 Mar. 2025].

[8] GAIA-X European Association for Data and Cloud AISBL. (n.d.). What is GAIA-X? Available at: https://gaia-x.eu/ [Accessed 3 Mar. 2025].

the event of cyberattacks, political crises, or domestic infrastructure failures.[9] Unlike traditional data centers or commercial cloud storage, data embassies are established through bilateral agreements between the home and host countries, granting them special legal protections akin to diplomatic embassies. This means that the data stored within remains subject only to the laws of the home country, not the host country. The concept of a data embassy is based on the fact that it is a network, and the data is not stored only in one location. Thanks to the multilocation factor, the data embassy helps to mitigate or, at the very least, distribute the risk of losing critical data.

Data embassies could fundamentally reshape the future of global data governance, offering nations a secure and legally protected method of storing sensitive digital information. As cyber threats grow more sophisticated and geopolitical tensions escalate, more countries may adopt data embassies as part of their national security strategies.[10] Importantly, this concept should not be confused with terms like "e-embassies" or "digital embassies" as used by actors such as the United States, which typically refer to virtual platforms that replicate consular services without establishing a physical diplomatic mission. A more comparable example, in terms of existential stakes, is Tuvalu's recent move to digitize its national identity. As a small island nation at risk of disappearing due to rising sea levels, Tuvalu has begun archiving its governmental data, history, and cultural records online, a symbolic and practical attempt to preserve the country's legacy. The data embassy model could prove especially relevant and appealing for Tuvalu as it explores pathways to digital survival.

Beyond individual state initiatives, international organizations such as the European Union and the United Nations may play a role in standardizing legal frameworks for data embassies, ensuring their protection under international law.

Further than their role in ensuring digital sovereignty and cybersecurity, data embassies offer significant economic and strategic advantages for both the home and host countries. On an international level, data embassies can be leveraged as diplomatic and economic assets, in fact, host countries that agree to house a foreign nation's data embassy benefit from closer diplomatic ties, increased technological collaboration, and potential

[9] Luxembourg Ministry of Digitalisation. (n.d.). Data Embassy Initiative. Available at: https://innovative-initiatives.public.lu/initiatives/data-embassy. [Accessed 3 Mar. 2025].

[10] Fernandez, M. (2023). Towards a New International Framework for Data Governance: Proposing Data Embassy Status for Global Data Centres. SSRN. Available at: [http://dx.doi.org/10.2139/ssrn.4991958] [Accessed 3 Mar. 2025].

economic incentives. By attracting data embassies, host nations position themselves as trusted digital hubs, enhancing their reputation as secure, politically stable, and technologically advanced nations. This can encourage foreign investment in cloud services, cybersecurity industries, and digital infrastructure projects, fostering long-term economic growth.[11]

For businesses operating within a country that hosts data embassies, the presence of high-security, government-controlled data centers can create new opportunities in the cybersecurity and IT sectors, for example companies specializing in encryption, data protection, and cloud storage management may find new markets by offering supporting services to data embassies, stimulating local innovation and job creation.[12] Additionally, as data protection laws become stricter worldwide, governments may start requiring private sector data storage to follow similar models, leading to new business opportunities for cloud providers willing to align with data embassy frameworks.

From a geopolitical standpoint, data embassies enable nations to strengthen alliances through digital cooperation, much like traditional embassies do in diplomacy. A country that entrusts its most critical data to a specific ally reinforces bilateral ties and increases strategic interdependence, making digital infrastructure an integral part of international relations. In the future, we may even see regional data embassy networks, where nations within political blocs, such as the European Union, ASEAN, or BRICS, establish mutual data protection agreements to ensure sovereignty and security across borders. If widely adopted, this model could help create a more resilient, decentralized and sovereignty-respecting global digital infrastructure.[13] While the concept of data embassies has its origins in Europe, it holds considerable appeal for states in the Global South, many of which are becoming increasingly dependent on digital infrastructure for the management of critical state functions.[14] This relevance is amplified by the growing risks of ex-

[11] Deloitte. (2022) Digital sovereignty and economic growth: The role of secure data infrastructure. Available at: https://www2.deloitte.com/global/en/insights/industry/technology/digital-sovereignty.html [Accessed 25 Feb. 2025].

[12] Gartner. (2021) Strategic planning for cloud sovereignty: The future of data protection and business expansion. Available at: https://www.gartner.com/en/insights/cloud-sovereignty [Accessed 5 Mar. 2025].

[13] World Economic Forum. (2021) The geopolitics of data: Why sovereignty matters. Available at: https://www.weforum.org/reports/the-geopolitics-of-data [Accessed 5 Mar. 2025].

[14] International Telecommunication Union (ITU). (n.d.). ITU cybersecurity work programme for developing countries. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf. [Accessed 5 Mar. 2025].

ternal interference, especially from technologically dominant states in the Global North, in sensitive domains such as national elections and democratic processes.[15]

## I.II Historical Background and Evolution of the Concept

Long before the advent of digital governance and cloud computing, states developed strategies to protect, archive, and restrict access to their most critical records. From ancient imperial archives to modern-day state-controlled digital infrastructure, the methods of preserving national information have continuously evolved in response to technological advancements, geopolitical threats, and national security concerns.

The necessity of controlling national information increased importance as international relations developed, with the rise of diplomacy in the medieval and early modern periods, states began to store and transmit sensitive political, military, and economic information beyond their borders. In response, embassies became critical hubs for secure communication and data storage, much like modern data embassies today. During the Renaissance, the Republic of Venice maintained highly classified diplomatic archives that recorded foreign trade negotiations, espionage operations, and intelligence gathered from rival states. European monarchies in the sixteenth and seventeenth centuries relied on complex encryption techniques to protect diplomatic messages from interception. The development of coded correspondence systems enabled sovereign states to exchange classified information securely, establishing early principles of data confidentiality and controlled access to sensitive state information.[16]

By the nineteenth century, as nation-states consolidated their power and expanded their bureaucratic institutions, the need for large-scale data management systems became even more pressing. The British Census Act of 1801 introduced one of the first thorough government-led census programs, requiring the systematic collection and archival storage of demographic data. Meanwhile, the United States established the National Archives in the early twentieth century to protect its most critical legal, military, and intel-

[15] Fruhwirth, M. (2023, July 17). Tackling foreign election interference through self-determination. Völkerrechtsblog. Available at: https://voelkerrechtsblog.org/tackling-foreign-election-interference-through-self-determination/. [Accessed 5 Mar. 2025].

[16] Mallett, M.E. & Hale, J.R. (2006). The Military Organization of a Renaissance State: Venice, c. 1400 to 1617. Cambridge University Press. Available at: https://doi.org/10.1017/CBO9780511562686. [Accessed 5 Mar. 2025].

ligence documents.[17] This period saw the emergence of state-run, centralized archives, which governments protected under strict security measures, ensuring that no foreign power could access or manipulate their national records.

By the mid-twentieth century, with the advent of computing technologies, governments transitioned from physical document storage to digital data management. The introduction of mainframe computers and early data-processing systems allowed states to digitize tax records, military intelligence, and census data. One of the earliest large-scale implementations of government-controlled digital data storage occurred in the 1960s when the United States Social Security Administration developed one of the first computerized databases for managing citizen records. In France, the 1980s saw the introduction of the Minitel system, a government-run digital network designed to provide public access to state information while ensuring data integrity and protection.

As the internet expanded in the 1990s, governments worldwide began shifting their administrative services online, a process that led to new challenges regarding digital security and sovereignty. For instance, Estonia emerged as a pioneer in e-governance, launching the X-Road platform in 2001, which enabled secure government data exchanges and set the foundation for fully digital public administration. Around the same time, Singapore developed a national e-government action plan to digitize state services while protecting national data from cyber threats. Despite these innovations, governments faced increasing difficulties in managing and securing the vast amounts of data they collected. The cost of maintaining domestic data centers was prohibitively high, and many countries lacked the expertise to operate such infrastructure independently. This led to a growing reliance on third-party technology providers, particularly multinational cloud computing companies, to store and process government information.[18]

The rise of cloud computing in the early twenty-first century transformed the way governments stored and accessed their data. Instead of relying solely on nationally controlled data centers, many governments turned to cloud services offered by global technology giants such as Amazon Web Services (AWS), Microsoft Azure, and Google

[17] Posner, R. A. (1972). Archives and the Public Interest: Selected Essays by Ernst Posner. Washington, D.C.: Public Affairs Press. Available at: http://files.archivists.org/pubs/free/ArchivesInTheAncientWorld-2003.pdf. [Accessed 5 Mar. 2025].

[18] Camp, L.J. (2000). Trust and Risk in Internet Commerce. Cambridge: MIT Press. Available at: ISBN 9780262531979. [Accessed 5 Mar. 2025].

Cloud. These cloud providers offered unprecedented efficiency, scalability, and cost savings, making them attractive alternatives to state-run data centers.

However, as governments became increasingly dependent on foreign-owned cloud storage, concerns over data sovereignty and security emerged. Many nations realized that their most sensitive data, ranging from military intelligence to citizen records, was stored on servers located in foreign jurisdictions and governed by foreign laws. During this period, countries began reconsidering their approach to digital sovereignty, leading to new initiatives aimed at securing national data, such as France's "Cloud de Confiance" (Trusted Cloud) initiative, designed to ensure that critical government data remained under strict state control. [19]

Despite these efforts, national data centers remained vulnerable to cyberattacks, geopolitical instability, and natural disasters and governments recognized the need for a more secure solution, one that would allow them to retain full control over their data while mitigating the risks associated with both domestic infrastructure failures and foreign legal constraints.[20] It was in this context that the concept of data embassies emerged, a new model that applied diplomatic-style protections to digital infrastructure stored in a foreign county.

## I.III Why Countries Adopt Data Embassies: Estonia and Bahrain

Data Embassy is a concept that emerged quite recently, but there is a country that due to several reasons that will be discussed shortly, has been successfully adopting this solution since 2017, this country is Estonia. Many could think of Estonia as a country with a fragile economy, still struggling from political tensions and big cultural differences, akin to other former-URSS countries. Reality is very far from this assumption, in fact, Estonia has consistently sought to redefine itself in the digital sphere, transcending its geographical limitations through bold and innovative technological advancements. Whether this is through the recent decision to store every citizen's healthcare records on

[19] European Commission. (2021). Digital Public Services and Interoperability: The Evolution of E-Government in the EU. Brussels: European Union Publications Office. Available at: https://digital-strategy.ec.europa.eu/en/library. [Accessed 5 Mar. 2025].

[20] Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company. Available at: ISBN: 978-0-393-35217-7. [Accessed 6 Mar. 2025].

an immutable, verifiable blockchain, or the rather bold attempt of amassing 10 million e-Residents by 2025, Estonia's status as a digital vanguard is rarely disputed. The country's transformation since regaining independence in 1991 has been extraordinary, in many ways the collapse of the Soviet Union gave Estonia a rare opportunity of a fresh start, free from political legacy. A young, forward-thinking government capitalized on this moment, laying the foundation for a technology-driven state.[21]

A key milestone in Estonia's digital revolution was the launch of Tiger Leap (Tiigrhüpe) in 1996, an initiative that drove rapid advancements in both digital infrastructure and education. This period marked a profound economic, social, and political transformation, as Estonia embraced technology as the key to streamlining state institutions and fostering innovation. Unlike larger nations with extensive legacy systems, Estonia lacked substantial infrastructure, forcing it to adopt a digital-first approach. This commitment to technological progress resulted in a steady rollout of cutting-edge e-governance solutions, including the eID system in 2002, i-Voting in 2005, and e-Health in 2008. These advancements significantly improved public services, efficiency, and security, eventually leading to the creation of the e-Estonia brand, a concept the government actively promotes to the world as a model for digital transformation.

Today, Estonian citizens enjoy seamless access to a vast array of e-services. Voting can be done online, tax filing takes few minutes to complete, and nearly all medical prescriptions are processed electronically, reducing administrative burdens on the healthcare system. Estonians often joke that the only things one cannot do online are getting married or divorced. At the core of this ecosystem is X-Road, a groundbreaking Estonian innovation that serves as the backbone of the country's digital infrastructure. This system enables secure, encrypted data exchanges between government databases, registries, and services, allowing them to function interoperably within a decentralized network. X-Road ensures that Estonia's e-services operate seamlessly, efficiently, and most importantly, securely.

However, Estonia's reliance on digital infrastructure comes with significant challenges. Many critical databases and registries, such as the Land and Population Registers, exist solely in digital form, without physical copies to serve as backups. This raise pressing

[21] United Nations E-Government Survey. (2022). Estonia: A Model for Digital Governance. New York: UN Department of Economic and Social Affairs. Available at: https://publicadministration.un.org/egovkb/. [Accessed 6 Mar. 2025].

concerns for the government: Could Estonia's public administration continue to function in the event of a large-scale cyberattack? What if the country's territorial sovereignty were suddenly threatened? For Estonians, these are not hypothetical questions, but real and valid concerns shaped by history.[22]

In fact, In the spring of 2007, Estonia was victim of three weeks of large-scale Distributed Denial of Service (DDoS) cyberattacks, widely considered the first ever major case of cyber war. These attacks, seemingly orchestrated by pro-Russian individuals and hacker groups, targeted governmental, political, financial, and public service websites, severely disrupting the country's access to the internet.

The attacks were seen as a retaliation against the Estonian government's decision to relocate a Soviet-era war memorial, the Bronze Soldier, in Tallinn. Following protests from Estonia's Russian-speaking minority, the cyberattacks escalated into what appeared to be a deliberate and highly coordinated offensive. Up to two million pre-infected botnets across 175 countries launched a massive, synchronized attack, overwhelming Estonian online services with data floods. While 174 nations assisted Estonia in countering the crisis, Russia refused to cooperate, denying involvement and claiming it too had been targeted in a minor cyber incident.

The attacks were strategic and dynamic, adjusting to countermeasures and stopping at precise moments and synchronized with other hostile Russian actions, such as the abrupt suspension of commercial rail links under the pretext of "repairs."

Estonia faced big economic loss estimated to be in the billions of Euros, however, despite the disruption, Estonia's resilience and international support helped mitigate the damage. The stability of key Estonian innovations, such as Skype, and rapid assistance from NATO and allied nations, ultimately reinforced the country's cybersecurity capabilities and global reputation. While there were concerns that public trust in the government's ability to defend against unconventional threats might erode, the swift and coordinated response prevented widespread discontent. Notably, the attacks did not appear to exacerbate internal divisions between Estonia's ethnic and linguistic communi-

[22] Heller, M. (2017). The Estonian Data Embassy Initiative: Protecting Digital Infrastructure from Modern Threats. Royal Holloway, University of London. Available at: https://pure.royalholloway.ac.uk/ws/portalfiles/portal/28736263/Network_Security_Article_Estonian_Data_Embassy_Initiative.pdf. [Accessed 6 Mar. 2025].

ties, highlighting the country's ability to withstand both digital and geopolitical pressure.[23]

Estonia has learned from past experiences that digital resilience is as crucial to national security as physical defenses, reinforcing its commitment to building a secure and sovereign digital future.

As a result, in 2013 the Estonian government launched the Data Embassy Initiative (DEI), a strategic and innovative solution designed to safeguard its digital infrastructure beyond national borders. The initiative was developed in response to the real possibility that Estonia might need to maintain its government functions and digital services from outside its own territory. The primary objective, as stated by the Estonian government, is to guarantee digital continuity, the ability of the state to preserve and operate its essential services and data, regardless of disruptions or external threats.[24] This approach ensures that Estonia's critical databases, registries, and digital services can remain operational even in extreme circumstances, including scenarios where the country loses access to its own territory.[25]

The Data Embassy Initiative is structured around three essential components designed to ensure the uninterrupted functioning of Estonia's e-government services. The first involves storing backups and maintaining live digital services within Estonia's own territory, strengthening domestic data security. The second focuses on hosting backups at Estonian embassies or in designated data centers located in allied countries, offering an additional level of protection against geopolitical risks. The third component involves using public cloud services operated by private companies to store non-sensitive data, ensuring further redundancy. Regarding the second approach, which involves the establishment of data embassies, the initiative focuses on securing additional data center resources through bilateral agreements with allied nations. Under this framework, the Es-

[23] NATO Strategic Communications Centre of Excellence (StratCom COE). (n.d.). Cyber Attacks Against Estonia 2007. Available at: https://stratcomcoe.org/pdfjs/?file=/publications/download/cyber_attacks_estonia.pdf?zoom=page-fit. [Accessed 5 Mar. 2025].

[24] MEAC (2016). Transforming digital continuity: Enhancing IT resilience through cloud computing, Ministry of Economic Affairs & Communications and Microsoft, Tallinn. Available at: https://www.digar.ee/viewer/en/nlib-digar:280707/252096/page/1. [Accessed 6 Mar. 2025].

[25] Microsoft & Republic of Estonia. (2016). Implementation of the Virtual Data Embassy Solution: Summary Report. Microsoft Corporation. Available at: https://download.microsoft.com/download/5/5/B/55B89687-C789-43DE-A5B1-89D9CE6BCF71/Implementation%20of%20the%20Virtual%20Data%20Embassy%20Solution%20Summary%20Report.pdf. [Accessed 6 Mar. 2025].

tonian government would effectively lease server space within pre-existing data centers, while ensuring that these designated areas remain under Estonian jurisdiction. This arrangement is designed to function similarly to traditional embassies, where the principle of extraterritoriality applies, granting the data embassy legal protections comparable to those outlined in the Vienna Convention on Consular Relations (1963). [26]

On June 20th, 2017, it was announced that the first data embassy would be located in Betzdorf, Luxembourg, after a bilateral agreement (the first of its kind) was signed by both heads of state. Since 2018, Estonia's 'cloud' extension has been housed in LuxConnect's certified Tier IV data centers. Tier IV certification signifies that the data center meets the highest international standards for reliability, redundancy, and resilience, capable of withstanding power failures, natural disasters, and cyber threats.[27] Estonia's decision to establish its first data embassy in Luxembourg was not arbitrary but rather a calculated choice based on geopolitical, legal, and technological factors. One of the primary reasons Estonia selected Luxembourg was its strong commitment to data sovereignty and cybersecurity. Luxembourg has long positioned itself as a leader in digital infrastructure, hosting several EU institutions' data centers and serving as a key player in Europe's secure data economy. Furthermore, Luxembourg's geopolitical stability made it a reliable choice for hosting Estonia's data embassy.[28] Unlike other potential host countries that may be more exposed to political instability or cybersecurity vulnerabilities, Luxembourg offers a neutral, secure environment, minimizing the risks associated with geopolitical conflicts or foreign state-sponsored cyberattacks.

Estonia showed the world the benefits of the first ever Data Embassy and paved the way to other countries which might want to implement this solution. In fact, other countries have already implemented Data embassies like for instance Monaco, India, Ukraine and Bahrain, each one with some minor or major difference from Estonia's one. For the pur-

[26] Heller, M. (2017). The Estonian Data Embassy Initiative: Protecting Digital Infrastructure from Modern Threats. Royal Holloway, University of London. Available at: https://pure.royalholloway.ac.uk/ws/portalfiles/portal/28736263/Network_Security_Article_Estonian_Data_Embassy_Initiative.pdf. [Accessed 6 Mar. 2025].

[27] LuxConnect. (2018). Tier IV Data Centers and Their Role in National Security Strategies. Luxembourg: LuxConnect. Available at: https://www.luxconnect.lu/. [Accessed 6 Mar. 2025].

[28] Heller, M. (2017). The Estonian Data Embassy Initiative: Protecting Digital Infrastructure from Modern Threats. Royal Holloway, University of London. Available at: https://pure.royalholloway.ac.uk/. [Accessed 10 Mar. 2025].

pose of our analysis, the Bahrain example is probably the one that deserves more attention since they adopted the model in a unique and interesting way. In 2018, the Kingdom of Bahrain implemented the Legislative Decree No. 56 of 2018 In Respect of Providing Cloud Computing Services to Foreign Parties ('Cloud Law'), this initiative aligns with Bahrain's goal of becoming a regional leader in cloud computing, while also challenging traditional boundaries of data sovereignty and jurisdiction. What makes this legislation particularly innovative is that it enables individuals and organizations to store data in Bahrain while ensuring that their data remains subject to the legal framework of their home country. This approach is particularly attractive to multinational corporations, financial institutions, and governments that require highly secure, geopolitically stable, and legally compliant data storage solutions. Regarding jurisdiction, Section 3 of the legislation explicitly states that the stored data, referred to as "customer content," will be governed by the laws of the country where the data owner is based, ensuring both regulatory flexibility and the benefits of Bahrain's advanced cloud infrastructure.[29] Bahrain's data embassy initiative is closely tied to the country's broader Vision 2030, a national economic strategy launched in 2008 to transform Bahrain into a diversified, sustainable, and knowledge-based economy. In fact, Bahrain seeks to move away from oil dependency and create a thriving digital economy that can compete with other Gulf states like Saudi Arabia and the UAE.[30] While Estonia pioneered the state-controlled data embassy model, Bahrain has taken a different approach, leveraging public-private partnerships, unlike Estonia's data embassy, which involve government-to-government agreements, Bahrain's initiative focuses on attracting foreign entities, both public and private. Bahrain's data embassy initiative is closely tied to its strategic partnership with Amazon Web Services (AWS), which has played a pivotal role in developing Bahrain's national cloud infrastructure. The country became the first in the Middle East to fully adopt a cloud-first policy, ensuring that government data, e-services, and critical national records are securely hosted within AWS-operated data centers. This collaboration enables Bahrain to provide cutting-edge cloud computing services while

[29] Anna-Maria Kolessova. (2023). Estonia's Data Embassy Initiative: A Framework for Building Cyber Resilience in Other Countries. Tallin University of technology. Available at: https://digikogu.taltech.ee/et/Download/dae125ad-ef19-4f5b-b087-305bdfc2aed2. [Accessed 10 Mar. 2025].

[30] Bahrain eGovernment Portal. (n.d.). Bahrain's Digital Transformation and Cloud Strategy. Government of Bahrain. Available at: https://www.bahrain.bh/wps/portal/en/. [Accessed 18 Mar. 2025].

maintaining sovereign control over critical data assets.[31] Unlike Estonia's government-controlled data embassy, Bahrain's model depends on a foreign cloud provider, which means it is still subject to external legal frameworks such as the U.S. CLOUD Act (2018). Ensuring long-term digital independence will require Bahrain to diversify its partnerships, potentially integrating multiple cloud providers or developing a sovereign cloud infrastructure in line with its Vision 2030 objectives.

From a geopolitical perspective, Bahrain's model offers a unique alternative to traditional data embassies. By relying on commercial cloud providers rather than government-controlled physical infrastructure, Bahrain avoids the diplomatic complexities associated with establishing extraterritorial data centers. However, this approach also raises questions about long-term data sovereignty, as reliance on foreign cloud service providers could potentially expose national data to foreign legal claims or influence. To address this concern, Bahrain has implemented strict data localization requirements, ensuring that all sovereign government data remains within Bahrain's borders, even when stored on cloud platforms. However, there is limited publicly available evidence indicating that foreign governments have fully embraced Bahrain's data embassy model in the same way Estonia has implemented its physical data embassy in Luxembourg.

## I.IV The Saudi Arabian Global AI Hub

The completion of this thesis coincides with a key development in the dynamic field of data embassies. On April 14, 2025, Saudi Arabia's Communications, Space and Technology Commission (CST) released a consultation draft of a "Global AI Hub Law." This initiative marks a pivotal milestone: Saudi Arabia stands out as the first G20 nation to introduce a legislative framework which formally integrates the idea of data embassies. The draft law acknowledges data embassies' strategic value while presenting a detailed plan to promote investment and establish governance and operational frameworks for sovereign data storage facilities outside national borders. By taking this action Saudi Arabia establishes itself as a leader in digital sovereignty initiatives which demonstrates

[31] Amazon Web Services (AWS). (2019). AWS Middle East (Bahrain) Region Now Open: Expanding Cloud Services in the GCC. AWS Public Sector Blog. Available at: https://press.aboutamazon.com/2017/9/amazon-web-services-announces-the-opening-of-data-centers-in-the-middle-east-by-early-2019. [Accessed 10 Mar. 2025].

the growing belief that secure data infrastructures play a vital role in national security and digital economic success. A comprehensive understanding of the draft legislation requires examining its position in relation to Saudi Arabia's overall strategic vision. The Kingdom's historical investments in technology produced inconsistent outcomes. The Kingdom of Saudi Arabia invested $45 billion into SoftBank's $100 billion Vision Fund which resulted in high-profile stakes in failed companies including the defunct real estate firm WeWork and the unsuccessful robotic pizza company Zume.[32] However, Saudi Arabia has recently adjusted its approach to technological development through a significant recalibration process. A new national priority has developed under Vision 2030 which positions artificial intelligence and data infrastructure as fundamental components for economic diversification. By merging regulatory initiatives with international partnerships and substantial investments, the Kingdom actively works to develop the essential infrastructure required for AI and related technologies. Saudi Arabia's efforts to develop emerging technologies extend beyond technology into geopolitical realms in order to decrease its reliance on oil revenues while also positioning itself as a leading force in the region and globally. For example, Google Cloud made an announcement in January 2023 about a newly established cloud region in Dammam which will provide high-performance low-latency services to various users including public sector institutions, large enterprises and both small and medium-sized enterprises as well as start-ups.[33] Additionally, in January 2025 AWS (Amazon Web Services) announced the opening of a new CloudFront region in Jeddah, created to distribute "basic" services like web content, applications, and data, such as images, videos, APIs, and websites to users with low latency and high transfer speeds with and expected investment of over 5 billion in the long run.[34] Oracle, a global technology company specializing in enterprise software, cloud infrastructure, and database solutions, has followed a similar path with

[32] Satariano, A., Saudi Arabia spends billions to build an A.I. industry from scratch (2024), The New York Times, 19 March. Available at: https://www.nytimes.com/2024/03/19/business/saudi-arabia-investment-artificial-intelligence.html. [Accessed 28 Apr. 2025].

[33] Google Cloud, Google Cloud expands regional presence with opening of Dammam cloud region, forecast to boost economy by USD 109 billion by 2030 (2023), Google Cloud Press Corner, available at: https://www.googlecloudpresscorner.com/2023-11-15-Google-Cloud-Expands-Regional-Presence-with-Opening-of-Dammam-Cloud-Region-Forecast-to-Boost-Economy-by-USD-109-Billion-by-2030. [Accessed 28 Apr. 2025].

[34] Amazon Web Services (AWS), New edge location in the Kingdom of Saudi Arabia (2025), AWS News. Available at: https://aws.amazon.com/it/about-aws/whats-new/2025/01/new-edge-location-kingdom-saudi-arabia/. [Accessed 28 Apr. 2025].

the launch of a cloud region in Riyadh, as part of its planned USD 1.5 billion investment to expand cloud infrastructure across the Kingdom. Notably, these are public cloud regions, meaning that any eligible customer can access and deploy services, leveraging advanced infrastructure while meeting local performance and compliance needs. This model is particularly significant as it enables big tech players to retain control over growing volumes of data, while simultaneously reinforcing their presence through localized investments aligned with national digital transformation goals. These are only few of the several examples that represent Saudi Arabia's strategy in becoming leader in the tech sector, objective that is set to be reached within 2030.

A fundamental shift, as mentioned at the very beginning of this subchapter, is the newly enacted Global AI Hub Law draft. The primary objective of the Law is to position the KSA as "a global digital hub and a pioneer in advanced technologies by fostering an attractive environment for foreign governments and private sector entities to develop and adopt such technologies for peaceful purposes and uses".[35] Developed by the National Competitiveness Center (NCC), the Istitlaa public consultation platform, launched in 2021, facilitates feedback from government bodies, commercial stakeholders, and the general public on proposed laws and regulations prior to their formal adoption. Since its inception, Istitlaa has played an instrumental role in shaping new legislation in the communications and technology sectors, enhancing regulatory transparency and fostering broader stakeholder engagement. The new legislation entails three distinct 'hub' models providing data hosting in the KSA, namely Private hub, Extended hub and Virtual hub. The hubs described are essentially data centers, or isolated and clearly demarcated parts of a data center. For what concerns the Private hub, it is a data center located within Saudi Arabia that is used exclusively to store and manage the data, applications, infrastructure, and services of a Guest Country ("A foreign state that enters into a Bilateral Agreement with the Kingdom to establish a Private Hub"), and is operated solely for that country's use under its own laws and regulations. The Law explicitly mention that the Kingdom will "recognize appropriate immunities and privileges for the staff, premises, communications, data and technology stack within the parameters and con-

[35] National Competitiveness Center (NCC), Global AI Hub Law – Final Draft for Public Consultation (2024), Istitlaa Platform, available at: https://istitlaa.ncc.gov.sa/en/transportation/citc/globalailaw/Documents/Global%20AI%20Hub%20Law%20EN-AR%20-%20Final%20Draft%20for%20PC.pdf. [Accessed 28 Apr. 2025].

sistent with the principles of the relevant international treaties.[36] Similarly, the Extended Hub model operates in the same way but is directed to Operators (hence private actors) rather than Guest Countries (public-governmental actors). Thus, both models allow the foreign state or entity to apply the laws of the country in which it is based. Furthermore, both models, similarly to the Estonia-Luxembourg case, require the parties to enter a bilateral agreement with KSA to operate, which is defined as an international agreement concluded between the Kingdom and a foreign state and subject to international law and in accordance with the Bilateral Agreement. Lastly, under the Virtual Hub model, foreign state or entities operating in Saudi Arabia can choose to apply the legal system of another country ("Designated Foreign State") to govern the customer content they host. This includes any data, applications, software, or media (such as text, images, video, or audio) stored, transmitted, or processed through the hub. Once a legal regime is designated, that content falls under the exclusive jurisdiction and authority of the courts and public institutions of the chosen country. However, only the legal systems of countries where the customer is legally domiciled or incorporated can be designated for this purpose. Under the Virtual Hub model, the Kingdom retains the right to "take action" under either domestic or international law whenever its authorities "reasonably considers" that the act of hosting or processing customer content "could constitute, a harmful act against the Kingdom or any other state or a form of interference in the internal affairs of another state." In addition, the proposed legislation sets forth clear termination provisions for the Global AI Hub framework. It grants the Council of Ministers, or its designated authority, the power to terminate any agreement, bilateral arrangement, or other related commitments, or to cancel any approval previously granted, in order to protect the KSA's safety, national security, and sovereignty, or if the Kingdom ceases to maintain diplomatic relations with a Guest Country.[37] In the event of a termination of a hub arrangement, the legal provisions would remain in effect for a period of 120 days from the official date of termination, or for a longer duration if stipulated in the termination notice, in order to ensure a smooth transition and enable the orderly migration of data

[36] National Competitiveness Center (NCC), Global AI Hub Law – Final Draft for Public Consultation (2024), Istitlaa Platform, available at: https://istitlaa.ncc.gov.sa/en/transportation/citc/globalailaw/Documents/Global%20AI%20Hub%20Law%20EN-AR%20-%20Final%20Draft%20for%20PC.pdf. [Accessed 28 Apr. 2025].

[37] Pinsent Masons, Saudi Arabia strengthens data sovereignty through draft AI hub law (2024), Out-Law News. Available at: https://www.pinsentmasons.com/out-law/news/saudi-arabia-data-sovereignty-ai-hub-law. [Accessed 28 Apr. 2025].

and services to alternative hosting environments. The draft legislation also calls for the establishment of a dedicated competent authority tasked with overseeing and enforcing the implementation of its provisions. Moreover, the Law explicitly states that none of its clauses shall be construed in a manner that would compromise the Kingdom of Saudi Arabia's safety, national security, diplomatic relations, or sovereign interests.

Each of the three hub models introduced in the Global AI Hub Law is designed to attract a distinct category of actor: the Private Hub is intended for sovereign use by foreign states; the Extended Hub is designed for foreign private sector operators and the Virtual Hub is targeted at Saudi-incorporated service providers serving international clients. Among these, the Private Hub most closely resembles the concept of a data embassy, as it enables a foreign government to manage its own digital infrastructure within Saudi territory under its domestic legal framework, it requires a bilateral agreement between two sovereign states and immunities and privileges consistent to international treaties are mentioned. However, it is fundamental to underline that even if the Law enables the creation of data embassy-like model, it does not create them itself. Nonetheless, the Private Hub model within the Global AI Hub Law enables the creation of arrangements that may functionally resemble a data embassy, if and only if the resulting Bilateral Agreement includes provisions akin to those found in diplomatic treaties, such as immunities, host-state non-interference, and extraterritorial application of law. However, because the law itself does not codify those protections, and leaves their scope to be negotiated case by case, Private Hubs cannot be assumed to enjoy the same level of legal data embassies, at least for now. A key nuance in the Extended Hub model is the requirement for a bilateral agreement between the Kingdom and the foreign state where the private operator is domiciled. While the operator is a private entity, the legal framework governing its activities must be endorsed and formalized through this state-to-state agreement, effectively making the foreign government a regulatory backstop that assures the operator's compliance with applicable laws and international standards. This structure adds a layer of diplomatic accountability that distinguishes the Extended Hub from ordinary commercial hosting arrangements.

Among the three models introduced in the Global AI Hub Law, the Virtual Hub model stands out as the most legally and conceptually innovative. Unlike the Private and Extended Hubs, which rely on bilateral agreements and foreign legal frameworks tied to

the operator or government, the Virtual Hub enables a Saudi-incorporated service provider to offer cloud or data services that are governed by the laws of a Designated Foreign State, specifically, the jurisdiction where the customer is domiciled or incorporated. This introduces a unique form of "jurisdiction-as-a-service", in which different clients hosted on the same infrastructure can be governed by different legal regimes, effectively decoupling physical geography from legal jurisdiction. It challenges traditional notions of data sovereignty and territoriality by allowing foreign legal frameworks, such as the GDPR, to apply within Saudi territory under controlled conditions. Crucially, this framework does not exclude foreign cloud providers; companies such as Amazon Web Services or Google Cloud could, in theory, establish a subsidiary in Saudi Arabia, obtain authorization under the Law, and then operate a Virtual Hub that applies, for instance, EU data protection law (such as the GDPR) for European clients. This opens the door to multi-jurisdictional compliance within a single physical infrastructure, a model that balances the Kingdom's desire for data sovereignty and regulatory oversight with the operational realities of global digital service delivery. Unlike rigid localization laws that often deter foreign investment and cross-border collaboration, the Virtual Hub model promotes interoperability, legal modularity, and trust-building in international data flows, marking a significant departure from sovereignty-based data control frameworks.

Surely, the Global AI Hub Law represents an innovative and ambitious legal framework for cross-border data governance and foreign digital infrastructure within the Kingdom, but it is also clear that its implementation raises a number of important legal, operational, and geopolitical questions. A closer examination of the law's provisions reveals several areas of ambiguity and potential tension, particularly regarding jurisdictional authority, enforcement mechanisms, and the stability of international cooperation.

More specifically, each of the three hub models allows, to varying degrees, for the application of foreign law within Saudi Arabia and in all three cases, the law introduces mechanisms that detach physical jurisdiction from legal jurisdiction, effectively creating quasi-extraterritorial zones within the Saudi digital ecosystem.

Despite this legal openness, the law simultaneously reinforces the Kingdom's ultimate sovereign authority through a series of override provisions. For instance, article 9(1) of the draft law allows the Council of Ministers, or its delegated authority, to terminate any

agreement, approval, or hub arrangement if it is deemed necessary to protect national security, public safety, or sovereignty, or in the event of a breakdown in diplomatic relations with a Guest Country. This termination can be executed unilaterally, without the need to prove breach or contractual failure, thus it becomes fundamental to draft a bilateral agreement that clarifies this issue, clearly defines a mechanism for termination and doesn't leave room for blank spots that might undermine sovereignty. Furthermore, Article 8(6) empowers the Kingdom to "take action" under Saudi or international law where its authorities "reasonably consider" that customer content hosted or processed in a Virtual Hub "could constitute a harmful act against the Kingdom or any other state or a form of interference in the internal affairs of another state."[38] This language is deliberately broad and discretionary, and its threshold, "reasonably considers", is low by international legal standards and practically allows the Kingdom to assert jurisdiction even over data nominally governed by foreign law. Nevertheless, can foreign actors truly rely on the legal autonomy it appears to offer? The answer is, at best, uncertain. While the law allows for the application of foreign laws and bilateral agreements, these operate within a framework that Saudi Arabia can unilaterally override in the name of state interest. This creates a model of "conditional legal autonomy", where the benefits of foreign legal application are permitted but not guaranteed.[39] This conditionality, in my opinion, undermines the predictability and legal certainty typically associated with international legal cooperation. For example, if a foreign state establishes a Private Hub in the Kingdom with expectations of sovereignty-like treatment for its data, but Saudi authorities later terminate the agreement due to a political dispute, the functional equivalence to a data embassy collapses. Similarly, in the Virtual Hub model, even if customer content is governed by foreign law, Saudi authorities may intervene under broad national interest grounds, creating possible conflicts between foreign data protection obligations and local enforcement actions. For governments and private entities considering long-term data infrastructure in Saudi Arabia, this tension introduces a degree of strategic and legal risk.

[38] National Competitiveness Center (NCC), Global AI Hub Law – Final Draft for Public Consultation (2024), Istitlaa Platform, available at: https://istitlaa.ncc.gov.sa/en/transportation/citc/globalailaw/Documents/Global%20AI%20Hub%20Law%20EN-AR%20-%20Final%20Draft%20for%20PC.pdf. [Accessed 28 Apr. 2025].

[39] Kuner, C., Transborder data flows and data privacy law (2014) Computer Law & Security Review, 30(1), pp. 104–108. Available at: https://doi.org/10.1016/j.clsr.2013.12.003. [Accessed 2 May. 2025].

A key structural feature of the Global AI Hub Law is its reliance on bilateral agreements between the Kingdom of Saudi Arabia and foreign states to authorize the establishment and operation of both Private and Extended Hubs. While this approach allows for tailored legal arrangements and diplomatic flexibility, it simultaneously raises serious questions about transparency, public oversight, and the potential for unequal or opaque regulatory treatment. The combination of state-to-state confidentiality and the absence of disclosure obligations in the law poses challenges to the development of a predictable and accountable digital governance framework. More in detail, the draft law states that the operation of both Private and Extended Hubs must be formalized through bilateral agreements between the Kingdom and the respective Guest Country. However, the law does not require that these agreements be published, registered with an international body, or subject to public or legislative review. In contrast to treaty-based digital infrastructure arrangements such as the Estonia-Luxembourg data embassy agreement, which was formally ratified and made publicly available, the Global AI Hub Law provides no procedural or legal mechanism for public transparency.

This lack of disclosure raises critical concerns: if legal regimes and operational terms are negotiated behind closed doors, stakeholders including civil society, regulators, and even domestic institutions, may be unaware of the rules governing how foreign actors process, store, or manage data in Saudi territory. Moreover, the absence of transparency creates the potential for unequal treatment, where similarly situated foreign partners receive different privileges or regulatory obligations based on the political or economic leverage they hold. The law's flexibility allows Saudi Arabia to grant or withhold access to the AI Hub regime on a case-by-case basis, guided by strategic, diplomatic, or commercial considerations. While this enables agility in international engagement, it also increases the risk of regulatory inconsistency, where decisions may be driven less by objective criteria than by geopolitical interest or negotiation dynamics.

In this context, larger economies or strategically aligned states may be able to negotiate more favourable terms, including greater data protection guarantees, more expansive operational control, or even de facto immunities. Conversely, smaller states or those with limited diplomatic leverage may find themselves bound by more restrictive or opaque agreements, reinforcing asymmetries in international digital power. Without

transparency, such disparities remain unchallengeable and unaccountable to domestic or international scrutiny.

These concerns undoubtedly offer important points for reflection for entities considering participation in the framework; however, further factors must be weighed to arrive at a comprehensive evaluation of its overall viability. One additional element to take into consideration is related to the so-called legal or forum shopping. In fact, Article 8(1) of the draft law states that a Service Provider incorporated in Saudi Arabia may offer Virtual Hub services in which customer content is governed by the laws of a Designated Foreign State.[40] The only requirement is that the customer be domiciled or incorporated in that foreign jurisdiction, and that the state be approved by the Saudi competent authority. However, the law does not articulate clear criteria for how such foreign states are to be evaluated or approved. This absence of transparency and standardization opens the door for forum shopping, in which Service Providers or customers may intentionally select jurisdictions with weak data protection laws, minimal oversight, or non-existent enforcement. This problem is not hypothetical: in the global cloud services market, it is already common for companies to route data through jurisdictions with favourable regulatory conditions, a practice that undermines the principle of meaningful user consent and weakens the protective function of national data laws.[41] The Law could unintentionally enable similar behaviour, unless further constraints or compatibility assessments are introduced. Regulatory arbitrage within the Virtual Hub model creates a dual threat: first, to user and customer rights, and second, to the credibility of the host state. If Service Providers select jurisdictions that lack effective data protection laws, or that do not uphold internationally recognized human rights and cybersecurity standards, users may unknowingly lose the protections they would otherwise enjoy under their domestic legal system. This erodes trust in the hosting infrastructure and may expose vulnerable populations or sensitive sectors (e.g., health, education, civil society) to privacy violations or state surveillance.

[40] National Competitiveness Center (NCC), Global AI Hub Law – Final Draft for Public Consultation (2024), Istitlaa Platform, available at: https://istitlaa.ncc.gov.sa/en/transportation/citc/globalailaw/Documents/Global%20AI%20Hub%20Law%20EN-AR%20-%20Final%20Draft%20for%20PC.pdf. [Accessed 5 May. 2025].

[41] Bradshaw, S., Millard, C. and Walden, I., Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services (2011), International Journal of Law and Information Technology, 19(3), pp. 187–223. Available at: https://doi.org/10.1093/ijlit/eaq017. [Accessed 7 May 2025].

At the same time, Saudi Arabia may be seen as facilitating regulatory avoidance, thereby attracting providers and clients who seek to circumvent stricter laws elsewhere. While this could offer short-term economic benefits, it risks reputational damage, diplomatic pushbacks, and even exclusion from international data transfer agreements or adequacy frameworks. To address this problem, other jurisdictions have introduced compatibility filters or legal adequacy reviews. For instance, the GDPR allows cross-border data transfers only to countries deemed to provide an "adequate level of protection," based on a comprehensive legal assessment.[42] Similarly, international organizations such as the OECD and APEC have developed cross-border privacy frameworks that include baseline standards to ensure interoperability without sacrificing enforcement.[43] The Global AI Hub Law lacks any equivalent mechanism, it does not require that the Designated Foreign State meet minimum legal, ethical, or procedural benchmarks, nor does it impose a system of tiered trust or oversight. This omission leaves the Saudi competent authority with unilateral discretion to approve jurisdictions, a structure that is both politically sensitive and legally vulnerable.

While the Global AI Hub Law positions Saudi Arabia as a legal innovator in the global digital infrastructure landscape, its ambitions must be viewed against a backdrop of geopolitical and technological constraints. Chief among these is the U.S. AI Diffusion Rule, introduced by the Biden administration in early 2025, which seeks to regulate the global export and deployment of advanced American AI technologies, including high-performance chips, foundation models, and training architectures. The rule, scheduled to come into effect on May 15, 2025, categorizes countries into three tiers, with only Tier One states granted unrestricted access to U.S. AI technology. Saudi Arabia is not currently included in this top tier, raising critical questions about its ability to realize the infrastructural demands of the very hubs it aims to operate under the Global AI Hub

[42] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Articles 44–46, Official Journal of the European Union, L119, pp. 1–88. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679. [Accessed 7 May 2025].

[43] APEC, Cross-Border Privacy Rules (CBPR) System Available at: https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf. [Accessed 7 May 2025].

framework.[44] The success of the AI Hub model, particularly the Virtual and Extended Hubs, depends on access to high-performance computing (HPC) infrastructure, advanced semiconductors (e.g., NVIDIA H100 GPUs), and cutting-edge AI models, most of which are currently developed and exported by U.S.-based firms. Saudi Arabia's exclusion from Tier One effectively places it in a restricted-access category, requiring licensing or potentially facing outright bans for key AI inputs. This exposes a central vulnerability: even with full legal autonomy to apply foreign laws and host foreign-controlled data, Saudi Arabia does not yet control the underlying technological stack necessary to support this vision. Legal sovereignty, in this case, cannot compensate for hardware dependency, rendering the Kingdom's AI ambitions susceptible to the shifting posture of U.S. export policy.[45]

As stated before, the Global AI Hub Law enables significant legal pluralism, allowing foreign laws to govern customer data through mechanisms like the Designated Foreign State clause in the Virtual Hub model. However, the U.S. Diffusion Rule makes clear that legal autonomy alone does not guarantee operational sovereignty.[46] For example, a European company may wish to deploy a Virtual Hub in Saudi Arabia to process data under GDPR, but if that deployment depends on U.S.-origin GPUs or transformer models subject to export licensing, the project may become infeasible or delayed. Thus, there is a growing gap between the regulatory flexibility offered by the law and the real-world limitations imposed by international technology control regimes. This decoupling of law and infrastructure exposes the AI Hub model to external veto power, a risk that must be critically considered in evaluating the model's sustainability. Beyond logistical and compliance challenges, Saudi Arabia's exclusion from Tier One under the Diffusion

[44] DGA Group, Saudi Arabia introduces a draft Global AI Hub Law (2024). Available at: https://dgagroup.com/insight/saudi-arabia-introduces-a-draft-global-ai-hub-law/#:~:text=Overview%20of%20the%20law,consultation%20until%20May%2014%2C%202025. [Accessed 7 May 2025].

[45] Binnendijk, A., Cohen, R.S., Frederick, B. and Geist, E., Mitigating Risks to the U.S. AI Innovation Ecosystem: Selective Decoupling and the AI Diffusion Strategy (2024), RAND Corporation. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3700/PEA3776-1/RAND_PEA3776-1.pdf. [Accessed 7 May 2025].

[46] U.S. Department of Commerce, Framework for Artificial Intelligence Diffusion, Federal Register, Vol. 90, No. 10 (15 January 2025), Document No. 2025-00636. Available at: https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion. [Accessed 7 May 2025].

Rule may also signal strategic mistrust from Washington. Whether motivated by security concerns, foreign policy alignment, or broader AI governance priorities, the decision could disincentivize Tier One jurisdictions or companies from locating sensitive operations within Saudi territory. Even if the legal regime appears permissive and well-structured, geopolitical perception matters. If Saudi Arabia is viewed as a geopolitically unstable or technologically constrained jurisdiction, foreign partners may question the long-term viability of hosting critical AI operations, particularly those involving dual-use technology, medical datasets, or government services. In this sense, the exclusion does not merely limit infrastructure acquisition; it affects the symbolic and strategic credibility of Saudi Arabia as a digital host state.

In conclusion, the U.S. AI Diffusion Rule underscores the essential distinction between regulatory design and systemic power. While Saudi Arabia's Global AI Hub Law offers a pioneering model for jurisdictional flexibility and cross-border legal interoperability, its effectiveness is ultimately bounded by geopolitical realities. As long as core AI infrastructure remains controlled by a small group of exporting states, including the United States, efforts to build legal sovereignty must contend with the technological dependencies and strategic vulnerabilities imposed by global AI supply chains. These limitations must be integrated into any serious evaluation of the law's global viability.

*As this thesis is being written, a major update concerning the AI diffusion rule took place during the day of 13th May 2025, in the occasion of the visit of President Donald Trump to Riyadh. USA and the KSA have entered a 1000 billion dollars agreement regarding space, defense, energy, digital infrastructures chips and AI. Trump eliminated the AI Diffusion Rule hence enabling Saudi Arabia to import chips form USA to develop their new digital hubs. In fact, Nvidia will sell more than 18,000 of its latest artificial intelligence chips (GB300 Blackwell) to Saudi company Humain, the new Saudi company for AI, announced the day before the visit of the USA president. In the multi-billion agreement are included 10 billion for AMD and 5 billion for Amazon to build cloud interface. These new agreements radically change the relationship with KSA and practically allowing the Kingdom to become one of the biggest players in the field of AI in the near future.*[47]

[47] The White House. 2025. Fact Sheet: President Donald J. Trump Secures Historic $600 Billion Investment Commitment in Saudi Arabia. May 13. Available at: https://www.whitehouse.gov/fact-

# II. Legal Implications and Regulatory Challenges

## II.I The Legal Foundations of Data Embassies

As previously outlined, data embassies undoubtedly represent a technological breakthrough, incorporating cutting-edge cryptographic protocols and advanced data storage infrastructure. However, their true innovation extends well beyond the realm of technology. Arguably, the most defining feature that distinguishes a conventional data center from a data embassy lies not in its technical sophistication, but in the legal architecture that underpins it. At the heart of the data embassy model is the imperative to shield sensitive governmental data from any unauthorized access, including by those physically responsible for the data center's operation and maintenance. This level of protection is made possible through a nuanced and multilayered legal framework that integrates international treaties and conventions, bilateral agreements, domestic legislation, institutional protocols, and regulatory guidelines. It is precisely this legal complexity that enables data embassies to function as sovereign digital extensions of the state, subject solely to the laws and jurisdiction of the home country, even when located abroad. This analysis will primarily focus on the Estonian model, as it remains the most advanced and clearly defined example of a functioning data embassy to date.

The bilateral agreement between Estonia and Luxembourg draws its legal foundation and conceptual framework from the Vienna Convention on Diplomatic Relations (VCDR). While the agreement establishes a unique legal regime tailored to the digital context, it is explicitly modelled on the VCDR's principles, particularly the doctrine of inviolability of premises and archives under Articles 22 and 24. Actually, Article 6(3) of the bilateral agreement explicitly states that "the Grand Duchy of Luxembourg shall grant the premises the same treatment as granted to diplomatic missions in respect of its official communications and the transmission of all its documents." This provision affirms that the data embassy is entitled to protections equivalent to those enjoyed by tra-

---

sheets/2025/05/fact-sheet-president-donald-j-trump-secures-historic-600-billion-investment-commitment-in-saudi-arabia/. [Accessed: 13 May 2025].

ditional diplomatic premises, particularly regarding the confidentiality and integrity of its communications. Such measures are to be considered appropriate if they offer the same level of protection as that offered by Estonia to mission premises of Luxembourg (an excellent example of the principle of reciprocity). This enhanced protective obligation may, in certain cases, such as when the mission is deemed especially at risk, require the deployment of constant security measures, including 24-hour police or military presence. The duty to uphold the inviolability of diplomatic premises, as well as the mission's documents and archives, is stringent: the receiving state is required to exercise due diligence and make every reasonable effort to ensure such protection.[48]

The legal implications of inviolability under diplomatic law operate on both negative and positive obligations. On the one hand, the receiving state, in this case Luxembourg, is strictly prohibited from entering or otherwise interfering with the functioning of the sending state's mission, namely Estonia's data embassy. On the other hand, it bears an affirmative duty to actively safeguard the mission's integrity and operation, which includes taking reasonable measures to prevent third-party interference, such as acts of violence or disruption. This dual obligation was notably underscored in the Tehran Hostages case, where the International Court of Justice (ICJ) found that Iran's failure to protect the United States embassy from being stormed by student militias constituted a breach of its international legal responsibilities.[49] The rationale for the principle of inviolability lies in the inherent vulnerability of a mission and its personnel when situated outside the territorial jurisdiction and protection of their home state. Applying this framework to the data embassy concept underscores the gravity of the receiving state's legal commitment to ensure that the extraterritorial digital infrastructure of the sending state is treated with the same level of protection as a physical diplomatic mission.[50] It is therefore evident that the premises of the Data Embassy are granted privileges and immunities that are, in substance, equivalent to those afforded to diplomatic missions, the

[48] Sierzputowski, B. (2019) 'THE DATA EMBASSY UNDER PUBLIC INTERNATIONAL LAW', International and Comparative Law Quarterly, 68(1), pp. 225–242. Available at: doi:10.1017/S0020589318000428. [Accessed 25 Mar. 2025].

[49] International Court of Justice (ICJ), 1980. United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment of 24 May 1980. ICJ Reports 1980, p. 3. Available at: https://www.icj-cij.org/en/case/64. [Accessed 25 Mar. 2025].

[50] Obiene, F.M., 2024. Diplomatic law reimagined: Appraising the risks and prospects of data embassies. Law School Policy Review. Available at: https://lawschoolpolicyreview.com/2024/01/23/diplomatic-law-reimagined-appraising-the-risks-and-prospects-of-data-embassies/. [Accessed 25 Mar. 2025].

principal distinction lies in the fiscal treatment of the premises: under the bilateral agreement, the sending state is not fully exempt from national, regional, or municipal taxes and duties related to the premises, whether owned or leased, except in cases where such charges constitute payment for specific services rendered.

It is not only the physical premises of a diplomatic mission that are deemed inviolable under international law, but also their contents, specifically, the "archives and documents of the mission," as affirmed in Article 24 of the VCDR. The Tallinn Manual *2.0*, that analyses how international law applies to cyber operations and cyber warfare, developed by legal and military experts under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence and that serves as a key reference for interpreting international legal norms in the digital age, offers a contemporary interpretation of that provision. It suggests that such inviolability extends to digital materials and devices, including computers, servers, storage drives, and other forms of information technology housed within the mission. Hence, this suggests that traditional embassies, already afforded robust protections under the VCDR, could in principle serve as secure locations for hosting data infrastructure to ensure continuity of government services. This legal foundation partly explains why Estonia initially considered leveraging its existing diplomatic missions for this purpose, viewing them as potential sites for safeguarding critical state data within the framework of established international law. In fact, for over a decade, Estonian critical databases were routinely backed up onto magnetic tapes and physically transported to various Estonian embassies via diplomatic pouches on a quarterly basis. This method, while operationally functional, underscored the need for a more modern, scalable, and secure solution, ultimately contributing to the conceptual development of the data embassy model.[51] This consideration is crucial to understanding the rationale behind Estonia and Luxembourg's decision to negotiate and conclude a bespoke bilateral agreement, one specifically designed to ensure that data embassies benefit from a robust legal framework and can operate with maximum efficiency and security. A key factor influencing this decision was the recognition that traditional embassy premises lack the stringent physical and technical safeguards required for housing

[51] Robinson, L., Kask, L. and Krimmer, R., 2019. The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis. In: Kerstin Martens et al. (eds.), Diplomacy in the Digital Age. University of Tartu. Available at: https://doi.org/10.1145/3326365.3326417. [Accessed 26 Mar. 2025].

critical state databases and managing sensitive digital infrastructure, protections typically afforded by high-tier data centers. From insufficient redundancy capabilities to vulnerabilities in existing telecommunications systems and limitations in on-site technical expertise, diplomatic missions were assessed as inadequate, and potentially even exposed, in the event of a crisis, whether occurring on Estonian territory or within the host country. Additionally, Estonia maintains only 37 diplomatic missions worldwide. Given the government's policy to establish such facilities only in politically stable and allied countries, the global pool of viable locations for secure data embassies would be inherently constrained. [52] Another motivating factor for establishing specially designated data embassies lies in the desire to pre-empt and mitigate any potential concerns or suspicions on the part of the receiving state. The presence of unusually sophisticated digital infrastructure within a traditional diplomatic mission could give rise to fears that such premises are being used for activities beyond the scope of recognised diplomatic functions. This perception could foster distrust and strain bilateral relations, an outcome that would go against to one of the core objectives expressed in the preamble of the Vienna Convention on Diplomatic Relations: the promotion of friendly relations among states.[53] Moreover, article 3 of the Convention outlines the core functions of a diplomatic mission, such as representing the sending state in the receiving state, protecting its interests, negotiating with the host government, and promoting friendly relations. These functions are inherently interpersonal and state-centric, designed to facilitate formal diplomatic engagement. The mere operation of a secure data storage facility, however critical to national governance, does not fall neatly within this framework, as it involves no active diplomatic representation, communication, or policy negotiation. As Dr. Sierzputowski observes, the drafters of the VCDR did not foresee the establishment of missions dedicated to housing digital infrastructure, and thus the Convention includes no provisions addressing the transfer or management of data systems by the receiving state, nor does it account for modern cybersecurity challenges. In light of these omissions, Estonia and

[52] Obiene, F.M., 2024. Diplomatic law reimagined: Appraising the risks and prospects of data embassies. Law School Policy Review. Available at: https://lawschoolpolicyreview.com/2024/01/23/diplomatic-law-reimagined-appraising-the-risks-and-prospects-of-data-embassies/. [Accessed 26 Mar. 2025].

[53] United Nations, 1961. Vienna Convention on Diplomatic Relations. 500 UNTS 95. Available at: https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf. [Accessed 26 Mar. 2025].

Luxembourg's decision to negotiate a dedicated bilateral agreement appears not only prudent but necessary.[54]

At this stage, it is reasonable to affirm that diplomatic law constitutes the principal legal foundation for data embassies. It is frequently noted that diplomatic law enjoys a relatively high level of compliance in comparison to other domains of international law. This can be attributed to the fact that, perhaps more than in any other area, the mutual advantages of adherence to diplomatic norms are both tangible and immediate. States are incentivized to respect these protections because they rely on the same privileges for the effective operation of their own missions abroad, reinforcing a culture of reciprocity and legal observance. However, it still remains an imperfect framework.[55] In practice, diplomatic law is inherently shaped, and often constrained, by the delicate balance of interests between the sending and receiving states, creating structural tensions that can give rise to legal and political ambiguities in novel contexts such as that of extraterritorial digital infrastructure.

## II.II Abuse of Diplomatic Privilege

Historical instances of abuse under the framework of diplomatic immunity raise important concerns that must be addressed when considering the legal safeguards surrounding data embassies. A pertinent example illustrating the potential for abuse of diplomatic privileges is the Equatorial Guinea v. France case before the International Court of Justice. In that instance, Equatorial Guinea unilaterally designated a building as part of its diplomatic mission in France, despite allegations that it housed material evidence linked to tax evasion, embezzlement, and corruption involving senior political figures.[56] Such scenarios exemplify the misuse of diplomatic protections, a risk explicitly anticipated in the Preamble of the Vienna Convention on Diplomatic Relations, which em-

[54] Sierzputowski, B. (2019) 'THE DATA EMBASSY UNDER PUBLIC INTERNATIONAL LAW', International and Comparative Law Quarterly, 68(1), pp. 225–242. Available at doi:10.1017/S0020589318000428. [Accessed 25 Mar. 2025].

[55] American Journal of International Law, (1985) THE ABUSE OF DIPLOMATIC PRIVILEGES AND IMMUNITIES: RECENT UNITED KINGDOM EXPERIENCE, Editorial Comment *641. Available at: https://www.ilsa.org/Jessup/Jessup07/basicmats/ajil_higgins_article.pdf. [Accessed 27 Mar. 2025].

[56] Immunities and Criminal Proceedings (Equatorial Guinea v. France), Judgment, I.C.J. Reports 2020, p. 300. Available at: https://www.icj-cij.org/case/163. [Accessed 27 Mar. 2025].

phasises that diplomatic immunities are intended to facilitate the performance of official functions, not to serve individual interests or shield unlawful conduct.[57]

In the digital realm, similar concerns have been raised by experts contributing to the Tallinn Manual, who warn that the use of a diplomatic mission's cyber infrastructure to disseminate espionage tools or malware into the receiving state constitutes a clear abuse of diplomatic function (p. 211). As digital infrastructure becomes more central to state operations, the risk that it may be repurposed for covert or malicious activities, including cyberattacks against third states, becomes increasingly significant. Accordingly, any extension of diplomatic privileges to data embassies must also account for the possibility of their misuse, reinforcing the need for carefully calibrated legal safeguards and accountability mechanisms.[58] N.P. Ward provides a compelling analysis of the mechanisms available to states when diplomatic privileges are misused, particularly the doctrine of forfeiture and the persona non grata provision enshrined in Article 9 of the Vienna Convention on Diplomatic Relations (VCDR). Traditionally, these tools have been used to expel diplomats engaged in espionage or activities incompatible with their status, such as the systematic misuse of embassies for intelligence operations, as seen in multiple Cold War incidents. Although the persona non grata designation presupposes the presence of individuals, Ward's broader point is that abuse of privileges, especially when directed against the interests of the host state, may justifiably result in a retraction of immunity and removal from the host territory.

Applied to the context of data embassies, the question arises: what happens if a state misuses an extraterritorial digital facility not to conduct diplomacy, but to engage in cyber operations, political interference, or illicit surveillance under the cover of inviolability? While no diplomatic personnel may be physically present, the digital infrastructure itself could be subject to analogous scrutiny. If a data embassy were to violate the terms of its bilateral agreement or international law, for example by hosting cyberattack infrastructure or refusing lawful transparency, the host state could invoke a functional equivalent of persona non grata, such as termination of the bilateral agreement, expulsion of the facility, or suspension of privileges. Indeed, the Estonia–Luxembourg

[57] United Nations, 1961. Vienna Convention on Diplomatic Relations. 500 UNTS 95. Available at: https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf. [Accessed 27 Mar. 2025].

[58] Obiene, F.M., 2024. Diplomatic law reimagined: Appraising the risks and prospects of data embassies. Law School Policy Review. Available at: https://lawschoolpolicyreview.com/2024/01/23/diplomatic-law-reimagined-appraising-the-risks-and-prospects-of-data-embassies/. [Accessed 26 Mar. 2025].

agreement includes dispute resolution (Article 8) and termination clauses (Article 10), which serve as legal exit routes in cases of misconduct. Ward's insights reinforce that diplomatic privilege is not absolute; it is conditional on peaceful and lawful conduct. Just as individuals may forfeit protection through abuse, so too might digital diplomatic infrastructures, especially as international law evolves to accommodate this new domain.[59]

The Estonia–Luxembourg agreement addresses the potential for misuse of the data embassy premises through a prudent legal safeguard expressed in Article 7, which states that the premises "must not be used in any manner incompatible with the purpose laid down in this Agreement or by other rules of international law."[60] This clause is particularly significant as it broadens the scope of regulation beyond the specific terms of the agreement itself to include general obligations under international law. By doing so, the drafters introduced a flexible yet robust standard that allows for the regulation of unforeseen or evolving scenarios, including potential abuses of privilege.

This approach contrasts with the VCDR, which provides a more narrowly defined list of permissible diplomatic functions under Article 3. Notably, the Estonia–Luxembourg agreement does not explicitly define the operational "purpose" of the data embassy, leaving its scope open to interpretation. While Estonia's public declarations offer guidance, suggesting that the facility is intended solely for the storage and protection of critical state data, the absence of a precise textual definition means that the prohibition in Article 7 serves as a crucial normative anchor. It ensures that the data embassy cannot be lawfully used for activities that would contravene either the spirit of the agreement or broader international legal standards, including those concerning cybercrime, espionage, or unlawful data manipulation. Even so, the Estonia–Luxembourg agreement does not explicitly outline the legal consequences should a data embassy be misused to facilitate or promote cybercriminal activity. As mentioned earlier, Article 8 establishes a framework for dispute resolution, stipulating that any disagreement between the Parties concerning the interpretation or implementation of its provisions, if not resolved through negotiation or other mutually agreed means, shall be submitted to a specially convened

[59] Ward, I., 1977. Espionage and the forfeiture of diplomatic privileges. Journal of International Law and Policy, 5(3), pp.221–242. Available at: https://scholar.smu.edu/til/vol11/iss4/6. [Accessed 26 Mar. 2025].

[60] Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems. Available at: https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf.

arbitral tribunal. This tribunal, composed of three arbitrators, is to be constituted on a case-by-case basis, ensuring a neutral and binding adjudication process tailored to the specific circumstances of each dispute. This lack of specificity likely reflects the friendly nature of the bilateral relationship and the shared trust between Estonia and Luxembourg, where the likelihood of such abuse was considered minimal and potentially unconstructive to emphasize during negotiations.

However, this omission does not negate the inherent risks associated with granting extraterritorial protections to digital infrastructure. Rather, it suggests that the parties consciously accepted these risks as part of a calculated trade-off to enable a novel form of digital sovereignty. Notably, Article 10 of the agreement allows for the termination of the arrangement with 24 months' notice, providing a formal exit mechanism should the relationship deteriorate, or misuse occur. Crucially, the principle of inviolability, as established under Article 6 of the agreement, is designed to survive the termination of the data embassy itself, preserving the continued legal protection of the archives and information systems, much in the same way that the VCDR safeguards diplomatic archives beyond the life of a mission. This concern gives rise to yet another legal and ethical complication: the potential for a government to exploit the protected status of a data embassy to conceal politically sensitive information from public scrutiny or to obstruct access to material evidence by judicial authorities. Such concerns are not merely theoretical. The Equatorial Guinea v. France case exemplifies how diplomatic protections can be invoked to shield buildings and their contents from investigation, even when serious allegations, such as corruption or financial misconduct, are at stake. Similarly, in the Bancoult case in the United Kingdom, diplomatic privilege was cited to seek the exclusion of critical documents, originally obtained via WikiLeaks, that could have influenced the legal outcome.[61]

These examples demonstrate how diplomatic immunities may be repurposed to frustrate transparency or accountability mechanisms. Scholars such as Dr. Benvenisti and Dr. Lustig have noted that states increasingly employ international legal frameworks as strategic instruments in domestic political struggles, often to neutralize opposition or avoid

[61] R (on the application of Bancoult No 3) (Appellant) v Secretary of State for Foreign and Commonwealth Affairs (Respondent). Available at: https://supremecourt.uk/uploads/uksc_2015_0022_judgment_af89da8fbf.pdf.

institutional oversight.[62] Given this pattern, the potential for data embassies to serve similar ends, particularly when their contents are shielded by inviolability clauses, cannot be ruled out. This underscores the importance of balancing the functional immunities of data embassies with safeguards that prevent their misuse for undemocratic or obstructive purposes.

### II.III Further Legal Complexities

A further dimension of legal complexity arises when the continuity of government in the sending state is disrupted by political upheaval, such as a coup or contested leadership transition. A pertinent illustration is the 2021 military coup in Myanmar, where the military removed the elected government, leading to disagreement over the international recognition of the country's legitimate government.[63] The UN General Assembly, faced with conflicting claims to legitimacy, ultimately deferred recognition of a new representative. This scenario underscores the potential vulnerability of data embassies to similar disputes. In cases where a sending state's government is challenged or replaced, questions may arise as to who retains lawful access to the inviolable data stored abroad. Host states could be placed in a legally and politically sensitive position, having to determine which claimant has the authority to manage or retrieve the data embassy's contents. These contingencies highlight the importance of incorporating clear succession protocols, recognition clauses, and contingency governance frameworks within bilateral data embassy agreements, particularly when engaging with states prone to political instability or contested sovereignty.[64]

One aspect that remains somewhat ambiguous is whether Estonia is entitled to display its national flag and emblem at the data embassy premises. Although the bilateral agreement does not explicitly provide for this, such a right can be inferred by analogy from the principle of inviolability. Displaying national symbols may be deemed neces-

[62] Benvenisti, E. and Lustig, D., 2008. Reclaiming democracy: The strategic uses of foreign and international law by national courts. American Journal of International Law, 102, pp.241–274. https://doi.org/10.1017/S0002930000016704. [Accessed 26 Mar. 2025].

[63] McKenna, A. 2021 Myanmar coup d'état. Encyclopedia Britannica. Available at: https://www.britannica.com/event/2021-Myanmar-coup-d-etat. [Accessed 26 Mar. 2025].

[64] Obiene, F.M., 2024. Diplomatic law reimagined: Appraising the risks and prospects of data embassies. Law School Policy Re-view. Available at: https://lawschoolpolicyreview.com/2024/01/23/diplomatic-law-reimagined-appraising-the-risks-and-prospects-of-data-embassies/. [Accessed 27 Mar. 2025].

sary to publicly signal the premises' protected status and to reinforce their exemption from search, requisition, attachment, or execution under international law. This symbolic visibility serves not only a ceremonial function but also a practical legal purpose by ensuring that the premises are clearly recognised as enjoying special protections. Notably, the agreement affirms that even in situations of force majeure resulting in partial or complete disruption of communications, the premises are still entitled to the same preferential treatment as traditional diplomatic missions. This reinforces the understanding that the data embassy constitutes a distinct category within the broader notion of diplomatic premises, one specifically adapted to the unique requirements of digital sovereignty and extraterritorial data protection.[65]

While data embassies are frequently framed as pragmatic legal innovations designed to secure digital assets beyond national borders, they also function as instruments of strategic legitimation, particularly for small and technologically advanced states like Estonia. As Hafner-Burton, Helfer, and Victor (2009) argue in their work on the political origins of international law, states often adopt or promote legal instruments not solely for compliance or enforcement purposes, but to garner legitimacy, both domestically and internationally. Their analysis shows that states use legal agreements to signal credibility, gain support from allies, and pre-empt criticism or resistance to new or controversial policies. Estonia's bilateral agreement with Luxembourg is a compelling example of this logic in action. Drawing on Hafner-Burton's typology of international law as a tool of legitimation through legalization, Estonia's data embassy agreement serves to institutionalize its self-image as a digital leader committed to the rule of law in cyberspace. Much like how countries have used treaty commitments in human rights law to bolster democratic credentials or climate agreements to position themselves as environmentally responsible actors, Estonia uses the diplomatic-law inspired data embassy framework to frame its actions as legally coherent and normatively progressive. This move is not incidental. As Hafner-Burton explain using the example of post-Soviet countries joining human rights treaties they had no intention of fully implementing, legal instruments are often used as external signals to validate internal strategic directions. Estonia, a former Soviet republic still building its international identity, leverages the legal architecture of

[65] Sierzputowski, B. (2019) 'THE DATA EMBASSY UNDER PUBLIC INTERNATIONAL LAW', International and Comparative Law Quar-terly, 68(1), pp. 225–242. Available at: doi:10.1017/S0020589318000428. [Accessed 28 Mar. 2025].

the data embassy to differentiate itself from authoritarian models of digital governance, such as those promoted by Russia or China, and to reinforce its alignment with Western legal norms.

Moreover, this process of legitimation is not passive. As Hafner-Burton and her co-authors argue, international law-making is shaped by political entrepreneurs, states that seek to reshape or extend legal regimes to their advantage. By invoking diplomatic law in a novel context, applying the inviolability provisions of the Vienna Convention to digital infrastructure, Estonia does more than protect its data: it actively pushes the boundaries of international legal discourse, creating space for broader acceptance of digital sovereignty and the extraterritoriality of data protection. This mirrors Hafner-Burton's discussion of how states reinterpret existing legal norms (such as sovereignty or jurisdiction) in order to legitimate institutional innovations that reflect emerging technological or geopolitical realities.

In this way, Estonia's data embassy is not just a defensive legal shield, it is a performative legal innovation that aligns with the broader theory of how law is used to construct legitimacy, define appropriate behaviour, and frame state identity in a complex international environment. Understanding the legal basis of data embassies through this lens reveals not only their technical function, but also their role as vehicles of soft power, used to shape international expectations around digital governance, sovereignty, and cyber resilience.[66]

## II.IV The EPO Bilateral Agreement: An Important Precedent

In examining how the concept of data embassies is evolving beyond bilateral state agreements, particular attention should be given to recent developments involving international organisations. One such case, grounded in a unique legal arrangement between a European institution and its host state, illustrates how diplomatic-style protections are being extended to digital infrastructure in ways that echo, but also diverge from, traditional models. More specifically, this case regards an agreement made by the European Patent Organization (EPO) and the Grand Duchy of Luxembourg. In order to gain prop-

[66] Hafner-Burton, E.M., Helfer, L.R. and Victor, D.G., 2009. Political science research on international law: The state of the field. The American Journal of International Law, 103(3), pp.291–324. Available at: https://doi.org/10.2307/20685861. [Accessed 5 Apr. 2025].

er and complete understanding of the matter, is necessary to start from me origins of EPO. he European Patent Organisation was established under the 1973 Convention on the Grant of European Patents (CGEP). According to the Preamble of the Convention, the Contracting States committed to “strengthening cooperation among European states in the protection of inventions.” The EPO operates as a public international organisation with legal personality and is responsible for granting patents within Europe in accordance with the CGEP framework. In each Contracting State, the Organisation is vested with the broadest legal capacity available to legal persons under national law, which includes, among other powers, the ability to acquire and dispose of movable and immovable property and to engage in legal proceedings.

Since its inception in 1973, the CGEP has been ratified by 38 European states, including Luxembourg. Notably, Article 32 of the Convention stipulates that the European Patent Office must provide the Administrative Council and its designated committees with the necessary staff, premises, and equipment required for the effective execution of their responsibilities. While the Convention on the Grant of European Patents (CGEP) does not provide a definition of the term "premises", the issue is addressed in detail by the Protocol on Privileges and Immunities (PPI), which was adopted alongside the Convention. The PPI outlines the legal conditions under which the European Patent Organisation (EPO), including members of its Administrative Council, staff, and other individuals engaged in its official functions, shall benefit from the privileges and immunities necessary for the fulfilment of their duties within each Contracting State.

Under Article 1 of the PPI, the premises of the Organisation are declared inviolable, a protection further extended by Article 2, which affirms that the Organisation’s archives and all documents in its possession or custody are similarly inviolable and exempt from any form of requisition, confiscation, expropriation, or sequestration. In a manner closely resembling the Vienna Convention on Diplomatic Relations, national authorities are prohibited from entering EPO premises without the consent of the President of the European Patent Office, except in urgent circumstances, such as fire or disaster, where entry is necessary to carry out protective measures. Additionally, Article 4(1) of the PPI provides that the Organisation, within the scope of its official activities, shall be exempt from all direct taxation on its property and income. In terms of communication rights, the EPO is entitled, in each Contracting State, to receive the most favourable treatment

available to any other international organisation, including the secure transmission and handling of its official documents and correspondence. The Protocol on Privileges and Immunities also authorises the Administrative Council of the European Patent Organisation to enter into complementary agreements with one or more Contracting States in order to give practical effect to the provisions of the Protocol and to safeguard the Organisation's operational interests.

Exercising this prerogative, on 5 March 2018, the EPO and the Grand Duchy of Luxembourg concluded a Complementary Agreement specifically concerning the inviolability of the Organisation's archives. While Article 2 of the PPI already affirms the inviolability of EPO archives and documents, this agreement extends the scope of that protection to explicitly include digital and electronically stored data.

Article 1 of the Complementary Agreement stipulates that the protections under Article 2 of the PPI apply to the EPO's entire archives, encompassing not only physical materials such as correspondence, manuscripts, photographs, and recordings, but also computer data, digital media, data carriers, and any other analogous materials, regardless of their location or custodian. Importantly, the provision ensures that both the substance and medium of the Organisation's data are covered, thereby adapting traditional concepts of inviolability to the realities of modern information systems and reinforcing the legal security of digital assets entrusted to EPO infrastructure in Luxembourg. The Administrative Council of the European Patent Organisation (EPO) explicitly justified the conclusion of the Complementary Agreement with Luxembourg by stating that such an instrument was necessary to safeguard the Organisation's interests in relation to the planned externalisation of its data centers. The Council noted that the existing wording of Article 2 of the PPI lacked the precision required to ensure adequate protection for electronically stored data, particularly when such data is held by third parties at locations outside the EPO's direct control. Although the agreement applies solely within the territory of Luxembourg, it represents a significant legal advancement in the treatment of digital archives.

In effect, the agreement establishes what has been described as the world's second "Data Embassy", extending enhanced legal protection to the EPO's digital infrastructure hosted on Luxembourgish soil. Uniquely, it also marks the first instance of a data embassy-type arrangement between an international organisation and a sovereign state. It is

important to note, however, that the Vienna Convention on Diplomatic Relations (VCDR) and the Vienna Convention on Consular Relations (VCCR) do not apply to the EPO, as the Organisation is neither a state nor a member of the United Nations or its specialised agencies, as required under Articles 48 VCDR and 78 VCCR. Nevertheless, the parties are free to draw inspiration from the principles and structures of those treaties when shaping bilateral agreements.

In this context, the Complementary Agreement stands out as a compelling example of legal innovation in the field of international data governance. It demonstrates how the concept of inviolability, traditionally applied to physical diplomatic premises and documents, can be effectively adapted to protect electronic archives through tailored legal instruments outside the conventional diplomatic framework.[67]

Following the landmark agreement between the European Patent Organisation (EPO) and Luxembourg, similar partnerships have emerged that further underscore Luxembourg's strategic position as a host of critical digital infrastructure. Notably, both NATO and the European Commission have established legal arrangements with Luxembourg for the hosting of their data and information systems. Although the limited information available, these agreements, while differing in structure and scope, similarly aim to ensure robust legal protection, operational resilience, and disaster recovery capabilities for extraterritorially hosted digital assets. For NATO, this is exemplified by the establishment of a joint data centre with its support agency (NSPA), which emphasizes redundancy and operational continuity in secure environments. Likewise, the European Commission launched a new data center in Luxembourg to consolidate its core digital operations and meet the growing demands of large-scale IT systems. While these arrangements do not adopt the precise terminology or model of a "data embassy," they demonstrate a shared institutional commitment to secure and sovereign digital infrastructure outside traditional diplomatic premises, reinforcing Luxembourg's role as a trusted jurisdiction for hosting sensitive digital environments.[68]

[67] Sierzputowski, B. (2019) 'THE DATA EMBASSY UNDER PUBLIC INTERNATIONAL LAW', International and Comparative Law Quar-terly, 68(1), pp. 225–242. Available at: doi:10.1017/S0020589318000428. [Accessed 9 Apr. 2025].

[68] Robinson, L., Kask, L. and Krimmer, R., 2019. The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis. In: Kerstin Martens et al. (eds.), Diplomacy in the Digital Age. University of Tartu. Available at: https://doi.org/10.1145/3326365.3326417. [Accessed 9 Apr. 2025].

# III. Case Study – Italy and SpaceX

## III.I Italy's Strategic Data and National Security Needs

Throughout this thesis, the concept of data embassies has served as a lens through which to examine how states navigate the tension between technological interdependence and sovereign control. The evolving concept of twenty-first century sovereignty now revolves around the idea that a nation can maintain jurisdictional command over digital structures across international boundaries. Yet, as this chapter turns its focus to Italy, it becomes evident that states are also confronting a different, more complex challenge: the issue now revolves around determining whether nations should and how they can surrender some control to international entities in return for operational benefits instead of claiming authority over overseas data. Emerging indications that Italy may be prepared to entrust components of its civilian and military strategic communications infrastructure to a non-EU private company raise urgent questions about the durability of traditional notions of digital sovereignty, most notably in the data governance and data protection. If data embassies represent an effort to assert sovereign control over data stored abroad, what does it mean when a country allows foreign privately operated systems, subject to the legal frameworks and strategic interests of another state, to become embedded in its core national communication systems? Is this a calculated trade-off in pursuit of resilience and capability, or does it risk subordinating sovereign functions to commercial or geopolitical interests beyond the state's reach?

This section examines the impact of such a strategic decision, presenting it as a modern-day counterpart to the data embassy paradigm, but in reverse: rather than projecting national power abroad, the strategic choice signifies the entry of foreign-dominated infrastructure into home space.

Before assessing the impact that entrusting national sensitive and strategic satellite communication and data storage systems to a third-party private actor, it is first necessary to examine how Italy has traditionally approached the governance of its most sensitive data flows across both civilian and military domains.

During the last ten years, Italy has worked extensively to enhance its national capabilities for storing and safeguarding critical information infrastructures while operating under its own legal jurisdiction. This strategic move represents a wider European initiative to reduce reliance on non-EU digital service providers while strengthening sovereignty over public and defense-related digital systems. Despite significant advancements, there are ongoing challenges especially at the point where resilience meets real-time mobility and military-grade interoperability. The Italian assessment of foreign-operated systems must be understood in the context of its developing framework for national digital sovereignty alongside operational restrictions.

Italy's idea of national digital autonomy is centered on the Polo Strategico Nazionale (PSN), its flagship program for the sovereign management of sensitive public data. The PSN was created as part of the Piano Nazionale di Ripresa e Resilienza (PNRR) from the recognition that hosting strategic public datasets, such as those pertaining to taxation, welfare, health, justice, and digital identity systems, on foreign or unregulated cloud services poses a national risk. Italy's dependence on non-EU cloud companies "undermines the ability of the state to ensure the confidentiality, availability, and integrity of public data in the long term," according to a 2021 AGID assessment.[69] The infrastructure includes multiple data centers located on Italian territory, certified to host classified data under Italian law and meeting compliance with ISO 27001, ENS, and EUCS standards for cloud security. While the PSN offers a safe, government-controlled alternative to American hyperscalers (such as AWS, Azure, and Google Cloud), its current focus is mostly civilian. The PSN, as stated by AGID and reiterated by the national cybersecurity agency (ACN), is meant to unify administrative and service platforms rather than to act as a theater-grade high-assurance military network.[70] This distinction is critical when determining whether new external capabilities, such as LEO (low earth orbit) satellite-based communication systems, should be pursued to address unmet national security requirements.

---

[69] Agenzia per l'Italia Digitale (AGID), Linee guida sull'accessibilità degli strumenti informatici della PA (2024). Available at: https://www.agid.gov.it/sites/agid/files/2024-06/Linee%20Guida%20sull%27accessibilit%C3%A0%20degli%20strumenti%20informatici%20-%20PA.pdf. [Accessed: 9 May 2025].

[70] Agenzia per la Cybersicurezza Nazionale (ACN), Strategia nazionale di cybersicurezza 2022–2026 (2022). Available at: https://www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf/81644476-f547-6a63-dda6-3356f4d1b2f6?t=1719931791748. [Accessed: 9 May 2025].

Italy has made major investments in space-based communications for defense purposes, primarily through the SICRAL satellite family. SICRAL (Sistema Italiano per Comunicazioni Riservate ed Allarmi) is managed by the Ministry of Defense and created in collaboration with Thales Alenia Space. It offers secure communications for the Italian Armed Forces and supports NATO missions through an interoperability framework. SICRAL-1b and SICRAL-2 (launched in 2009 and 2015, respectively) operate in geostationary orbit (GEO) and provide encrypted voice, fax, and data to naval, aerial, and ground systems. The 2019 agreement with France to co-invest in SICRAL 3 strengthens Italy's position in the EU and NATO space defense ecosystems.[71] Italy also contributes to Athena-Fidus, a Franco-Italian dual-use broadband satellite that serves both civil protection and institutional users. Furthermore, the country indirectly participates in the EU's new IRIS2 constellation, a flagship program to establish a secure LEO satellite communications system providing governmental-grade services among member states which is expected to deploy 290 satellites by 2027.[72] Nevertheless, these systems are shaped by the GEO satellite paradigm, meaning they are: expensive and slow to deploy, vulnerable to orbital targeting, limited in low-latency applications (critical in real-time combat scenarios), not built for mass civilian–military convergence, as expected in future multi-domain operations. This exposes a structural limitation: Italy's secure communications infrastructure, while operational and NATO-integrated, lacks the redundant, low-latency, transportable capability that is becoming increasingly important in today's cyber-kinetic war scenarios. This capacity gap is crucial to understanding why a durable, rapidly deployable LEO-based system like Starlink may be seen as a worthwhile solution.

Italy’s strategic data and communications posture cannot be fully understood without situating it within the broader context of European space and digital sovereignty frameworks, to which it is both a key contributor and beneficiary. Unlike smaller EU member states that may rely on external suppliers due to capability gaps, Italy is a systemic actor in Europe’s defense-industrial and space ecosystems, with the institutional, industrial,

[71] Telespazio, Space Alliance: follow-on contract signed with the Italian Ministry of Defence for SICRAL 3 (2020). Available at: https://www.telespazio.com/it/news-and-stories-detail/-/detail/space-alliance-follow-on-contract-sicral3. [Accessed: 9 May 2025].

[72] European Commission, IRIS² – Secure Connectivity (n.d.). Available at: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en. [Accessed: 9 May 2025].

and diplomatic means to influence the direction of EU policy in these domains. It is precisely this strategic placement that makes the potential outsourcing of sensitive communications infrastructure to non-EU private actors particularly consequential, not only for national autonomy but for Europe's collective ambitions. In fact, Italy has established itself as an essential player in European space governance through its active participation in both civilian and dual-use satellite missions. The European Space Agency (ESA) receives substantial funding support from Italy, which ranks third among its contributors behind Germany and France, leading to a major influence on Europe's unified space strategy. The Italian Space Agency (ASI), along with its industrial partners, demonstrates technological sophistication that parallels its financial and political commitments. ASI plays an essential role in managing Italy's participation within major European space programs. Their focus spans longstanding involvement in Galileo (EU global navigation satellite system) together with Copernicus (Earth observation program that supports environmental humanitarian and security monitoring functions) and the recent IRIS2 program, the European Commission's flagship secure satellite connectivity initiative offering an independent alternative to non-EU systems like Starlink. Italy's support doesn't revolve only around the financial aspect since it also holds technical leadership roles through its national industrial leaders like Leonardo, Thales Alenia Space Italia, Avio, and Telespazio. These companies offer sophisticated facilities to build satellites, launch services and process data and secure communication systems. The IRIDE constellation for instance demonstrates Italy's strategic influence within European space affairs through its leadership in the €1.1 billion Earth observation program developed under Italy's PNRR with ESA collaboration. The ASI-led IRIDE project will provide high-resolution multi-sensor satellite data for public and security applications through the major efforts of Italian companies. Through this initiative, Italy emerges as both a consumer and a principal designer and integrator of dual-use space technologies inside the EU framework.[73]

[73] Istituto Affari Internazionali (IAI) (2021) Space and European Digital Sovereignty: The Role of Italy. IAI Papers 21|11. Available at: https://www.iai.it/sites/default/files/iai2111_en.pdf. [Accessed: 10 May 2025].

## III.II Relying on Foreign Private Providers: Strategic and Legal Risks

As Italy seeks to strengthen its critical communications infrastructure through partnerships with external entities like SpaceX's Starlink service, a thorough analysis of dependency risks associated with third-country private operators is necessary. The integration of these platforms into national security communication systems creates intricate legal, strategic, and political vulnerabilities which surpass mere performance and bandwidth considerations. Such risks originate from the basic legal framework and geopolitical structure surrounding third-party providers as well as from the incompatible relationship between national security objectives and corporate management systems.

The main issue, being a provider such as Space X a U.S.-incorporated business, is that it is subject to U.S. export controls, operates under U.S. domestic law, and may be required to abide by directives from U.S. regulatory or intelligence agencies under frameworks like the CLOUD Act, the International Traffic in Arms Regulations (ITAR), or executive orders relating to national defense. This creates a jurisdictional asymmetry: even if Italy were to contractually govern service terms, the ultimate control over signal routing, system availability, or data prioritization may still rest with Washington. The situation presents serious sovereignty issues when facing crises or disagreements between Italy and US, scenario particularly relevant and quite likely to happen especially in the geopolitical uncertainty that is reigning worldwide in recent days, where the longstanding and consolidated alliance between EU Member States and U.S.A. does not look quite as solid as it used to be before. Should the U.S. government decide to suspend or restrict access to satellite services on grounds of its own foreign policy or export risk evaluations, Italy would have no guaranteed legal recourse, regardless of the contractual terms negotiated. The situation establishes a foreign actor's de-facto veto over Italian communications sovereignty, which contradicts both Italy's Strategia Nazionale di Cybersicurezza and the EU's developing doctrine for technological non-dependence.[74] Contractual fragility under duress poses the primary threat when strategic operations depend on private infrastructure facilities. Private contracts lack the treaty-

[74] Agenzia per la Cybersicurezza Nazionale (2022) Strategia Nazionale di Cybersicurezza 2022–2026. Available at: https://www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf. [Accessed: 10 May 2025].

based foundation of intergovernmental agreements and can be modified, paused or ended by service providers on their own accord, especially if compelled by national regulatory or security mandates. There is no structural assurance that Italian government communications would take precedence over more lucrative or politically favoured uses in a crowded or contentious communications environment.

Another overlooked risk factor is represented by the dual-use potential of satellite constellations such as Starlink. In fact, while ostensibly commercial, their deployment in U.S. Department of Defense for instance in missions across Ukraine and the Indo-Pacific region, turns them into essential geopolitical tools. Through reliance on these technologies, the Italian national infrastructure becomes part of foreign strategic systems which raises the potential for geopolitical backlash. In the event of escalation with a technologically advanced adversary (e.g. China), infrastructure like Starlink may be targeted by cyber, kinetic, or jamming operations, not just due to its military application but because of its visibility as a symbol of Western technological dominance. If Italy relies on such infrastructure for high-priority communications (military coordination, crisis response, civil protection), it must accept the reality that its communications infrastructure becomes more vulnerable, not less, to hostile targeting, precisely because it is hosted on a globally integrated, dual-use platform.

The assessment cannot be considered complete without taking into consideration the man behind Space X, a person that is increasingly tied with U.S. government and that holds more power and wealth than whole countries: Elon Musk. Donald Trump's second presidential term election and Elon Musk's appointment as leader of the new Department of Governmental Enterprise* (DOGE) transformed the connection between U.S. strategic assets and private sector innovation.[75] The operation of SpaceX's Starlink constellation under both a commercial license and strategic federal supervision poses new political risks and sovereignty challenges for countries that wish to adopt Starlink for their secure communications systems. Starlink's integration into US national strategy was already underway during the previous administration, as seen by its military appli-

*On day 29th May 2025, Elon Musk officially resigned from his role in the Federal Government after misalignments with Donald Trump over various matters, included tariffs and support in conflicts.

[75] Shear, M.D. and Conger, K. (2025) Trump Appoints Elon Musk to Lead New Federal Tech Office. The Washington Post, 2 February. Available at: https://www.washingtonpost.com/politics/2025/02/02/trump-musk-doge-appointment/. [Accessed: 10 May 2025].

cation in Ukraine, Taiwan, and the US Indo-Pacific logistics networks. However, since Musk's formal appointment to a cabinet-level position, the line between civilian tech entrepreneur and state actor has effectively blurred. It is essentially a strategic asset of the US federal government, deployed in accordance with American global interests and objectives. Because of this institutional entanglement, any Italian reliance on Starlink would expose it to the full range of US foreign and domestic policy decisions, particularly in areas where European and American interests are increasingly divergent, such as data regulation, defense industrial autonomy and tariff regimes.[76] Perhaps the most unexpected and dangerous aspect of Italy's prospective reliance on Starlink is the consolidation of strategic decision-making authority in the hands of a single individual, namely Elon Musk. This scenario is not merely theoretical or anecdotal: Musk now holds dual roles as both the de facto controller of Starlink through SpaceX and the head of the DOGE tasked with overseeing public–private tech integration and national innovation infrastructure, this consolidation of influence creates a condition of executive personalization that is at odds with the very foundations of democratic infrastructure governance. The control Musk holds over essential global communications networks stems from corporate ownership and personal influence backed by political connections rather than accountable institutional oversight. A perfect example is how the deployment of Starlink the Ukraine-Russia war actively influenced the conflict, not without contradictions and controversies. In February 2022, two days following Russia's full-scale invasion, Ukraine requested SpaceX to activate its Starlink satellite internet service in the country to replace internet and communication networks that had been damaged or destroyed during the conflict. Starlink has since been used by Ukrainian civilians, government officials, and the military for humanitarian aid as well as defense and counterattacks against Russian forces.[77] Later on, Musk denied allowing Starlink access to Crimea (a Russian-occupied territory in Ukraine), effectively preventing a Ukrainian attempt to launch a naval drone attack against Russian ships. His judgment, influenced by personal ideas on conflict escalation, effectively overruled a sovereign allied state's tactical au-

[76] European External Action Service (2025) EU–US Tensions Escalate Over Digital Tax and Tariff Disputes. EU Strategic Outlook Briefing No. 12. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1149. [Accessed: 10 May 2025].

[77] Wikipedia (2024) Starlink in the Russian-Ukrainian War. Available at: https://en.wikipedia.org/wiki/Starlink_in_the_Russian-Ukrainian_War. [Accessed: 13 May 2025].

tonomy during a war.[78] The situation demonstrated the vulnerability of infrastructure reliance on privately held, politically motivated systems: Musk operated not as a neutral service provider, but as a self-appointed geopolitical adjudicator. Additionally, Musk's public antagonism toward European digital sovereignty, environmental regulation and antitrust enforcement only sharpens this risk. Through his public platforms Musk repeatedly criticized EU measures like the Digital Services Act and the Cyber Resilience Act to establish himself as an advocate for deregulatory techno-libertarianism. Musk could potentially leverage his institutional power to restrict access to Starlink services or retaliate against EU and Italian policies that threaten his business interests or ideology. From a governance standpoint, this degree of personally mediated influence over key communications infrastructure brings an element of unpredictability that no public institution should be subject to. While nation-states typically interact with other states through treaties, mutual legal obligations, and diplomatic backchannels, dealing with Starlink under Musk effectively subjects national security to the logic of personality and private will, a framework free of procedural safeguards and structural impartiality. While Brussels works towards technological cohesion for the EU by focusing on digital sovereignty and space autonomy, Italy's decision to adopt a Musk-controlled U.S.-based system creates disunity and undermines the EU's leverage against both the U.S. and China. This would undermine Italy's credibility in programs like IRIS2 and IRIDE, as well as its industry participation in Copernicus and Galileo. Other member states may follow suit, resulting in a fragmented satellite communications regime across the Union, undermining efforts to unify shared encryption standards, bandwidth sovereignty, and legal jurisdiction over orbital traffic.

More recently, another degree of strategic ambiguity into the system's global footprint emerged: the possibility of Starlink satellites being used by Russian forces, either through capture, illicit resale, or third-party intermediaries. As reported by Forecast International, credible intelligence indicates that Russian-affiliated units may have gotten access to Starlink connectivity in occupied Ukrainian territory, despite SpaceX's stated

[78] Isaac, M. and Sanger, D. E. (2023) Elon Musk's Starlink Decision Disrupted a Ukrainian Attack. The New York Times, 7 September. Available at: https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html. [Accessed: 10 May 2025].

policy of restricting services to Ukrainian government users.[79] The Kremlin has not publicly confirmed such use, but intercepted communications and on-the-ground reports, which were initially disclosed by the Ukrainian Main Directorate of Intelligence, indicate that Russian military personnel have used Starlink to coordinate drone and infantry operations in frontline areas.[80] While SpaceX has denied any direct sales or authorizations to Russia, the episode highlights the difficulties of managing dual-use, commercially disseminated technology in high-intensity combat zones. Experts from the Ukrainian Security Service (SBU) together with cybersecurity analysts have conveyed concerns that Starlink's decentralized structure combined with its commercial distribution through third-party networks creates inherent vulnerabilities to misuse and diversions.[81] This vulnerability throws into question Starlink's reliability as a secure military communications infrastructure, particularly for NATO and EU members considering its integration. For nations like Italy, where data jurisdiction and strategic alignment are vital, the possibility of an adversary exploiting the same system utilized by NATO forces offers a fundamental security paradox, one in which resilience is acquired at the expense of exclusivity and legal confinement.

Furthermore, there's another clarification that I consider necessary to broaden the understanding of the topic and the scope of the assessment, namely the distinction between Starlink and Starshield. The first has been thoroughly discussed previously while the latter deserves few words, being unknown to most people. Starshield is a separate and classified division of Starlink, designed specifically for the U.S. Department of Defense and affiliated intelligence entities for military applications and is explicitly positioned as a sovereign U.S. government asset operating under U.S. military control. It was publicly announced in late 2022 and provides enhanced encryption, secure communications, and Earth observation capabilities tailored to defense applications. Unlike Starlink, which is generally openly distributed, its technology widely available in many jurisdictions, and

[79] Forecast International (2024) Potential Use of Starlink by Russia: A Background and the Implications, Defense & Security Monitor. Available at: https://dsm.forecastinternational.com/2024/05/15/potential-use-of-starlink-by-russia-a-background-and-the-implications/. [Accessed: 13 May 2025].

[80] Sanger, D.E. and Kramer, A.E. (2024) Ukraine Confronts New Security Threat as Russia Gains Access to Starlink. The New York Times, 24 May. Available at: https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html. [Accessed: 13 May 2025].

[81] Cyber Defense Magazine (2024) Cybersecurity Threats in Global Satellite Internet. Available at: https://www.cyberdefensemagazine.com/cybersecurity-threats-in-global-satellite-internet/. [Accessed: 13 May 2025].

its services, while capable of supporting military communications, are still based on a civilian-commercial contract structure, Starshield is not available to international partners or allied countries unless explicitly authorized by the US Department of Defense. Starlink and Starshield share the same satellite constellation's infrastructure and technology environment and are both part of SpaceX's low-Earth orbit (LEO), but they serve very different functions and are regulated by fundamentally different legal, operational, and strategic frameworks. The distinction between Starlink and Starshield architectures holds critical importance for Italy and other European nations evaluating Starlink integration into their national communication systems. While Starlink may appear appealing due to its operational resilience, mobility, and bandwidth benefits, it is not technically completely separate from the larger infrastructure used by Starshield, nor is it free of potential priority conflicts or strategic co-optation. In other words, even if allies employ Starlink terminals under commercial contracts, their functionality and signal channels are still managed by infrastructure that can be potentially reallocated or repurposed based on US defense priorities. It is important to emphasize that, in the event of a formal agreement between the Italian government and Starlink, both parties would, obviously and in principle, be bound by the terms set out in the contract. Ideally, Italy would be able to negotiate sufficient protections, however, given the current uncertainty of the global geopolitical landscape and the rapid, sweeping changes being implemented by the U.S. administration (whether for better or worse), it is prudent to consider a scenario in which one of the parties fails to uphold its obligations, particularly in the context of a conflict. It is also quite evident that the party most likely to breach the agreement would be the one holding greater leverage and control, which in this case would be the United States, potentially leaving the Italian side without effective recourse. Moreover, because Starshield is unavailable to international partners and is inextricably linked to US national security objectives, foreign reliance on Starlink creates an overall imbalance: while the US retains exclusive access to a hardened, sovereign-grade platform, its allies are left with a less secure, commercially governed version of the same architecture, which is potentially more vulnerable. In the event of conflict escalation, export control enforcement, or diplomatic tension, this two-tiered structure might severely disadvantage countries such as Italy, who may find themselves reliant on infrastructure that is not only operationally inferior but also jurisdictionally vulnerable. As

stressed before, Italy's national space and cybersecurity strategies mandate strategic autonomy and technological independence which makes it essential to develop sovereignty-preserving legal mechanisms like bilateral governance agreements and data jurisdiction clauses before engaging with U.S.-controlled satellite systems. Without appropriate safeguards Italy risks tying its essential communication systems to a U.S. military strategy through its use of Starlink.

### III.III Italy's Legislative Effort: the DDL Spazio

In light of these operational imperatives and jurisdictional vulnerabilities, the Italian government has taken steps to anchor its strategic autonomy in law. The deployment of foreign commercial systems like Starlink provides tactical benefits yet fails to address how sovereign control over communication infrastructure can be maintained without an established legal framework. The relevance of the Disegno di Legge per lo Spazio (DDL Spazio) becomes evident within this specific context. The Provvedimento "Disposizioni in materia di attività spaziali e di economia dello spazio", currently under parliamentary consideration, represents Italy's first dedicated legislative attempt to regulate its national space sector by integrating licensing and oversight with infrastructure planning and proposing legal mechanisms for sovereignty clauses in satellite cooperation between public and private entities. This section analyses how the DDL Spazio establishes state control over essential orbital infrastructure and explores its potential to form agreements similar to data embassies, which would allow Italy to utilize third-party service providers while maintaining its legal and strategic independence.

At its core, the DDL Spazio establishes a centralized administrative and regulatory structure for space operations, placing the Prime Minister's Office and the Italian Space Agency (ASI) at the helm of strategic decision-making. All entities involved in launch and satellite-related operations under Italian jurisdiction are required to register, and a licensing framework is outlined for both public and private operators, including international ones that collaborate with Italian actors. In this regard, the DDL Spazio has not yet developed a model comparable to the data embassy structures implemented by countries such as Estonia, whose bilateral agreements contractually guarantee jurisdictional sovereignty over digital infrastructure located abroad. However, certain provisions, par-

ticularly those in Articles 5, 6, and 14, may provide an enabling legal foundation for such arrangements. Article 5 allows the conclusion of international agreements with foreign governments and organizations for the co-management or co-hosting in the management of Earth observation infrastructure, with particular attention to ensuring maintenance costs are covered by commercially viable service models, while Article 14 highlights the strategic importance of maintaining control over space and communications assets that support vital national operations. According to these clauses, Italy might theoretically replicate a model akin to the Estonian data embassy, especially in situations where Italian sovereign interests are projected into infrastructure hosted abroad or, on the other hand, where a foreign infrastructure is located inside Italian territory but is subject to foreign law under explicit treaty-based guarantees. Digital sovereignty is not directly referenced in the DDL Spazio, yet its focus on national control and international agreements along with public-private partnerships implies that this development remains possible within the draft law's existing framework. The framework establishes Article 8 as a key component requiring government approval for any space-related activities conducted by public or private entities under Italian jurisdiction. The framework applies to foreign entities conducting operations on Italian soil or through collaborations with Italian firms. Authorization requires a formal evaluation process to confirm activity alignment with national interests and Italy's international obligations before any approval is granted. When legal jurisdiction, national security, or diplomatic priorities are at stake, this clause serves as a sovereignty filter, enabling the state to restrict or prohibit foreign involvement in essential infrastructure. Italy could now theoretically mandate specific data localization requirements, encryption protocols and legal jurisdiction conditions as prerequisites for approving satellite services under foreign control such as Starlink. The law thus equips Italy with the legal tools to shape agreements that retain sovereign enforceability, even when the infrastructure itself is operated by a third party. Article 9 supplements the pre-authorization mechanism by granting the Italian government the authority to suspend or cancel authorizations at any time if the activity is judged to be no longer in the country's best interests or if it violates public safety, order, or Italy's international legal commitments. This gives the state dynamic control over infrastructure dependencies, which means that even agreements that have already been granted can be legally undone if geopolitical conditions shift or if a partner

country engages in hostile behaviour. The termination clause mirrors the terms found in Saudi Arabia's Global AI Hub Law which enables Italy to establish comparable legal structures for protecting its strategic communication systems allowing Italy to renegotiate, suspend, or unilaterally terminate access to satellite-based services, including foreign-operated data centers or constellations, should those services be used in ways that contravene national security imperatives or diplomatic norms.

Furthermore, Article 24 of the draft states unequivocally that the State would support the rise of space activities as a catalyst for economic expansion, with a strong emphasis on equal and non-discriminatory access to national space infrastructure data, services, and resources. Crucially, Article 25 introduces the concept of a "riserva di capacità trasmissiva nazionale", a dedicated national satellite transmission capacity. This capacity, to be secured via satellite communications infrastructure, is to be managed exclusively by operators based in EU or NATO member states and is intended to guarantee continuity of service for public authorities in the event of cyberattacks, war, or terrestrial network outages. In addition, the clause does not limit this capability to infrastructure that is entirely owned by the Italian government; rather, it leaves open the prospect that such resilience could be guaranteed through international agreements or public-private partnerships, so long as jurisdictional and security guarantees are upheld.[82]

Despite its forward-leaning objectives and strategic ambition, the DDL Spazio, at its current draft stage, reveals significant gaps when evaluated against the imperatives of data sovereignty and secure infrastructure governance. Such omissions carry the risk of compromising the law's ability to function as a fully complete tool for defending national sovereignty in the digital and space domains. In the absence of complementary regulation or interpretive clarification, these weaknesses could translate into operational vulnerabilities, particularly in relation to data-intensive infrastructures such as Starlink or future sovereign constellation. The DDL Spazio's first and biggest flaw is that it makes no mention of data localization, either with regard to data held on ground-segment storage or via orbital relays. This absence stands in stark contrast to Italy's Strategia Nazionale di Cybersicurezza, which requires public administration and critical

[82] Camera dei Deputati – Servizio Studi (2024) Elementi di valutazione del DDL "spazio" (AC 163). Available at: https://www.camera.it/temiap/documentazione/temi/pdf/1472496.pdf?_1747318974496. [Accessed: 15 May 2025].

sectors to store data within Italian or EU jurisdiction.[83] The lack of integration between space law and this strategic cybersecurity plan indicates a policy inconsistency which could allow sensitive communications to pass through international infrastructure without enforceable legal oversight or physical control. Another weakness lays in the vague treatment of jurisdiction in public–private partnerships, particularly in scenarios involving foreign service providers. Although Article 9 offers revocation procedures and Article 8 empowers the state to monitor and approve space activities, foreign operators are not required to recognize that Italian law applies to the data or services provided through their platforms. This is particularly concerning when considering satellite constellations that provide cloud-based broadband access, like those run by Starlink, which may gather, transmit, and store massive amounts of encrypted data for both military and civilian use. The absence of specific jurisdictional requirements or localization rules leaves Italian authorities without legal means to influence data management choices after a contract has been executed and when the agreement falls under foreign legislation or U.S. export restrictions. When compared to European legal best practices, Italy's DDL Spazio's absence of specific clauses on data localization and jurisdictional enforcement is even more noticeable. A notable instance is the Space Operations Act of France, which creates a thorough system that mandates liability insurance, prior authorization, and jurisdictional filings for any satellite operation carried out from French territory. This law strengthens national sovereignty over space operations by guaranteeing that all missions are both expressly governed by French law and legally traceable.[84] At the supranational level, the European Union provides further regulatory models that could be adapted to the space domain. Both the NIS2 Directive and Articles 44 to 46 of the GDPR lay out clear requirements for cross-border data transfers, including adequacy assessments and binding corporate rules. These instruments offer well-established legal templates that could be embedded within Italy’s space law to ensure that data routed through or stored in satellite-linked infrastructures remains subject to enforceable jurisdictional oversight, yet these tools remain absent from the current draft of the DDL Spazio.

[83] Agenzia per la Cybersicurezza Nazionale (2022) Strategia Nazionale di Cybersicurezza 2022–2026. Available at: https://www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf. [Accessed: 15 May 2025].

[84] Legifrance (2008) Loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales. Available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000018931380/. [Accessed: 15 May 2025].

The parliamentary journey of the draft has not passed unnoticed by civil society and political commentators, the effort to finally regulate Italy's space laws and improve the nation's competitiveness in Europe's developing space economy has earned the DDL recognition, but it has also drawn a lot of criticism. Concerns range from ambiguous oversight mechanisms to provisions that may implicitly favour dominant non-EU tech actors, particularly SpaceX. One of the most frequently mentioned criticisms is that its current regulatory structure risks to legitimize asymmetrical partnerships, which allow foreign entities, particularly those with strong ties to non-EU governments, to function within Italian infrastructure ecosystems without sufficient reciprocal safeguards. For instance, the civic movement Meritocrazia Italia demanded immediate changes to prevent "leaving strategic infrastructures in the hands of uncontrolled private actors," citing the potential for businesses such as SpaceX to take advantage of the law's flexible framework to provide sensitive services with little to no public oversight.[85] Specifically, Article 25, which reserves satellite transmission capacity for companies domiciled in NATO or the EU, has come under fire for its omissions due to the lack of stricter provisions on jurisdictional enforcement, ownership transparency, or operational autonomy. These flaws make it possible for a multinational such as SpaceX to gain a strategic foothold through a nominally compliant European subsidiary, potentially bypassing the spirit of the national sovereignty clauses embedded in the draft. Furthermore, lawmakers from opposition parties have expressed concerns that the DDL Spazio's wording creates technological dependency risks and proposed amendments requiring mandatory public ownership of critical communication nodes, or at least a legal firewall preventing private operators from dictating service suspension terms. However, the government’s majority has stressed the importance of keeping the door open to foreign investment in order to accelerate the digital transition, pointing out that Italy lacks the industrial scale necessary to create a Starlink-equivalent on its own. This polarized reception demonstrates the bill’s ambiguous dualism: although it provides an opportunity for developing sovereignty-enhancing structures similar to data embassies, it also creates strategic vulnerabilities.

[85] Meritocrazia Italia (2024) D.D.L. Spazio: «Mi chiede misure volte a evitare che entità come SpaceX operino senza controlli adeguati». Available at: https://www.meritocrazia.eu/d-d-l-spazio-mi-chiede-misure-volte-a-evitare-che-entita-come-spacex-operino-senza-controlli-adeguati/. [Accessed: 16 May 2025].

## III.IV Policy Recommendations for Italy in Negotiations with SpaceX

The focus of this thesis on Italy's legal and strategic responses to extra-territorial satellite systems like Starlink demands an analysis of how legal instruments, such as the GDPR, are challenged by these new technologies. Drawing on interdisciplinary legal scholarship and technical infrastructure analysis, it becomes clear that Italy's national legal responses, including the DDL Spazio, are occurring in a context of systemic regulatory inadequacy, not only at the domestic level, but across the broader European legal order. The GDPR, widely considered one of the most robust data protection regimes in the world, is fundamentally structured around concepts of territoriality, legal jurisdiction, and transparent data flows. Each one of these assumptions are challenged by satellite-based networks such as Starlink. Orbital constellations rely on latency-driven routes, encrypted satellite-to-satellite relays, and continuously changing transmission channels, in contrast to terrestrial Internet Service Providers, which operate within distinct national areas and are governed by well-established licensing and auditing systems. The idea of "cross-border data transfers" is therefore ambiguous, if not completely inapplicable, since neither users nor regulators can accurately determine where data is being processed, stored, or transferred. Core GDPR concepts like "transfer" (Article 44), "appropriate safeguards" (Articles 46–47), and "establishment" (Article 3) are severely strained by this architectural opacity. The European Data Protection Board (EDPB), for example, has underlined repeatedly how crucial it is to guarantee "essentially equivalent" protection for personal data that is moved outside of the EU.[86] It might be impossible to determine whether data has ever crossed a jurisdictional boundary in the context of orbital data relays, let alone whether adequate safeguards were in place during the transmission. This leads to a situation known as a "jurisdictional vacuum," in which is the technological design, rather than legislative flaws, that weakens the GDPR's regulatory reach.

These findings, which are based on recent doctrinal research and regulatory guidance, suggest a more fundamental problem: legislation like the GDPR and the DDL Spazio

[86] European Data Protection Board (EDPB). (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en. [Accessed: 26 May 2025].

were designed for an internet that was based on territorial logic. They are ill-equipped to govern infrastructure that is physically detached from sovereign borders and algorithmically indifferent to them. Therefore, even with the best of intentions, Italy's legislative actions must be viewed as a response to a fundamentally changed environment, where sovereignty must be actively negotiated and defined through new legal mechanisms rather than being assumed through infrastructure alone. These insights point to a deeper structural issue: existing laws, including the GDPR and the DDL Spazio, were conceived for an internet built on territorial logic.

Current academic literature suggests a new approach known as "trusted orbital zones", which involves creating legal frameworks that assign specific orbital or ground-based infrastructure to fixed legal jurisdictions, despite the physical geography of data transmission. These zones would establish jurisdictional consistency, similar to data embassies, by maintaining legal oversight when infrastructure operations become shared or distributed.[87] Due to its established legal tradition and strategic geopolitical placement, along with its active participation in European and NATO security systems, Italy stands in a strong position to advance these developments. The concept aligns with the logic of Article 25 of the DDL Spazio, which calls for a "riserva di capacità trasmissiva nazionale," yet must be extended beyond NATO-aligned ownership to encompass jurisdictional guarantees over data itself.

An additional layer of complexity is added by a distinction between content and metadata, which is emphasized in GDPR interpretation and supported by ENISA guidelines. Even if content remains encrypted or anonymized, metadata such as routing paths, timestamps, or terminal IDs still qualify as personal data.[88] Thus, the DDL Spazio must guarantee that satellite services deployed for public or military communications not only comply with the GDPR requirements but also maintain auditability for metadata management and disclosure risks. This is particularly urgent when services are provided by actors strictly tied to foreign regimes such as SpaceX and the U.S. federal govern-

[87] Floridi, L., (2021). The data economy: Understanding the value of data and the regulation of the data market. Journal of Information Policy, 11, pp.26–41. Available at: https://doi.org/10.5325/jinfopoli.11.2021.0026. [Accessed 24 May 2025].

[88] European Union Agency for Cybersecurity, (2024). 2024 report on the state of cybersecurity in the Union: Condensed version. ENISA. Available at: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf. [Accessed 26 May 2025].

ment. These current challenges require Italy to take actions that move past the adjustment of its domestic laws. Through EU and NATO, Italy should advance the global standardization of legal frameworks that oversee satellite-based data systems by advocating for shared jurisdictional principles and enforceable standards of transparency and auditability. Italy has a unique potential to influence the next generation of frameworks for digital sovereignty because of its developing national cybersecurity policy, impending space law, and high-stakes international infrastructure negotiations. However, doing so will require both normative innovation and legal foresight, while the cost of delay is obvious: the loss of state sovereignty over its most important infrastructure in a world where boundaries no longer translate onto cables and satellites.

Given Italy's potential strategic partnership with SpaceX to enhance national communication systems for sensitive military and government operations, the development of a strong policy framework that protects national sovereignty becomes essential. This concluding section proposes specific recommendations to integrate the technological benefits of Starlink infrastructure deployment with the essential geopolitical requirement to ensure Italy’s legal autonomy and control over its data and communications systems. These recommendations are developed in response to the specific risks identified in previous chapters, namely the absence of data localization clauses in the DDL Spazio, the increasing concentration of infrastructure control in politically exposed corporate actors and the legal asymmetries inherent in cross-border data flows routed through privately operated satellite constellations.

First and foremost, any agreement between Italy and SpaceX needs to be drafted as a bilateral legal document grounded in public international law rather than merely a commercial contract. The agreement should be negotiated and ratified between the Italian state and the United States government or its appointed federal agency, and should not be limited to direct contractual engagements with SpaceX as a private corporation. This model would mirror the legal foundations of the Estonian–Luxembourg data embassy framework, which was explicitly codified through an international treaty rather than delegated to private contractual arrangements. Such a format offers greater legal resilience, enforceability and institutional continuity in the event of disputes or geopolitical changes. Additionally, it guarantees that Italy will not be left without remedies if

U.S. executive orders, shifts in federal policy or internal SpaceX leadership choices disrupt or limit Starlink services. With a bilateral treaty-based approach, Italy could embed clear jurisdictional provisions that would allow the Italian judiciary and cybersecurity authorities to exercise oversight over the service segments designated for governmental or military use.

It would be necessary, in my opinion, to include into the bilateral framework a formal "data embassy clause" to establish hardware nodes, transmission segments and edge infrastructure as sovereign extensions of the Italian State, outside from foreign jurisdiction and exclusively under Italian law. Such approach would not imply extraterritoriality in the traditional diplomatic sense but would introduce a degree of functional jurisdictional immunity over the infrastructure critical to state operations. The data embassy clause ensures that Starlink services remain uninterrupted and secure from surveillance or technical restrictions unless Italian institutions grant explicit prior authorization. The clause must be supported by enforceable continuity guarantees (i.e. minimum notice period and government authorization prior the suspension of the service), that mandate uninterrupted communication services for Italian authorities throughout crises, conflicts, or diplomatic breakdowns. Such provisions would help avoid situations like the one happened in Ukraine discussed previously in this thesis, when Elon Musk unilaterally cut off Starlink, highlighting the importance of contractual protections.

In addition to these legal safeguards, Italy must give infrastructure redundancy top priority. Even in emergency or backup situations, Starlink should not take over as the exclusive provider of institutional connectivity. Instead, it should be deployed as part of dual-path architecture where Starlink works either under or alongside the main terrestrial systems that have already been set up by the Polo Strategico Nazionale and will eventually (and optimistically) be integrated with European projects, like IRIS2. To prevent systemic dependency, Starlink's function should be restricted to providing additional resilience, and its services should be transmitted via Italian-controlled encryption and relay networks. Moreover, Italian-managed ground stations interacting with the satellite constellation, must be retained under state or EU jurisdiction ensuring that the data exchanged through Starlink is at all times subject to Italian cybersecurity policy and legal standards. The DDL Spazio, while silent on these specifics, does offer a useful foundation in this regard, with its clauses on strategic transmission capacity, licensing, and op-

erational control. However, a stronger data localization requirement is essential to ensure that all core data and metadata linked to this national reserve must be stored in infrastructure located within EU territory and governed by EU law. This would harmonize the provision with the Strategia Nazionale di Cybersicurezza and close the gap with GDPR principles on territorial enforcement.

A further recommendation would be that SpaceX should enter into strategic partnerships with Italy only with strict oversight controls in place. Italian authorities, including the National Cybersecurity Agency (ACN), should perform regular sovereignty compliance audits of SpaceX. The audits must evaluate the integrity of data routing and service continuity policies, alongside key management systems and contractual provision enforceability. A thorough examination of whether the services delivered through Starlink are technically or administratively entangled with Starshield is also necessary, considering its different and opaque governance model.

On top of that, Italy needs to understand that the SpaceX negotiations are more than just a bilateral matter. It is embedded within the larger framework of NATO interoperability requirements and EU digital policy. Therefore, Italy should work closely with Brussels to make sure that any deal with SpaceX complies with GDPR principles and the goals of the EU's Secure Connectivity Programme.

Italy must comprehend that sovereignty today is increasingly measured not by territorial contiguity but by control over infrastructures of communication, data processing and decision-making. Sovereignty, in this light, becomes “relational” and “operational”: the capacity of a state to shape or constrain the technical and legal conditions under which its citizens and institutions function.[89] The DDL Spazio, while a step toward asserting control, still operates within a legal paradigm that presumes territorial infrastructure as a precondition for regulation, resulting in inadequate protections.

Moreover, as stressed before, the current draft does not contain mandatory data localization requirements or extraterritorial jurisdiction clauses applicable to foreign service providers. It should be revised to include mandatory conditions for public–private partnerships involving non-EU operators. These conditions could take the form of a sovereignty impact assessment, a formalized review mechanism to evaluate whether any for-

[89] Catanzariti, M. (2024) Disconnecting Sovereignty: How Data Fragmentation Reshapes the Law, Springer. Available at: https://doi.org/10.1007/978-3-031-60734-9. [Accessed: 27 May 2025].

eign actor's involvement in Italy's digital or space-based infrastructure poses unacceptable risks to jurisdictional autonomy, operational resilience, or international alignment.

Compounding these challenges is the lack of an integrated European space law; even though individual EU member states, like France with its Loi sur les Opérations Spatiales, have started to regulate space activities with specific references to national security, liability, and licensing requirements,[90] the European Union as a whole still lacks a unified legal framework for space governance. The absence of harmonized EU legislation on space law not only weakens Europe's geopolitical leverage but also hampers the development of joint infrastructure governance tools such as trusted orbital zones or cross-border data enclave (data embassies).[91] By increasing EU-level involvement in space regulation, member states will gain better legal clarity and collective negotiation power when engaging with external providers while establishing jurisdictional protections within infrastructure procurement processes and interoperability standards. By doing so, sovereignty might be asserted on two levels: at the national level through bilateral treaties and domestic laws, and at the supranational level through technological standards, common norms, and strategic coordination. Only through a sovereignty model structured across several levels Italy can ensure that it does not merely lease foreign infrastructure, but governs it legally, technically, and politically.

[90] France. Loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales. Paris: Journal Officiel de la République Française. Available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000018931380/. [Accessed: 26 May 2025].

[91] Ars Interpretandi (2024) Dossier: Spazio e Diritto – Profili normativi del nuovo scenario spaziale europeo, Ars Interpretandi, 2/2024. Available at: https://www.arsinterpretandi.it. [Accessed: 26 May 2025].

# Conclusion

This study examined how contemporary challenges to digital sovereignty, jurisdictional enforcement and strategic infrastructure governance are impacting the legal and geographical boundaries of the modern state. By examining the legal model of data embassies and the implications of Italy's evolving space legislation, particularly the DDL Spazio, it is clear that "sovereignty needs to disconnect from physicality to pursue its objectives in a field such as data regulation" (Catanzariti, 2024), especially in the fields of cloud computing and satellite communication.

The study emphasized the diversity of legislative designs emerging to address the problem of data extraterritoriality by conducting a comparative examination of models such as Estonia's data embassy agreement with Luxembourg and Saudi Arabia's Global AI Hub Law. These examples show that, when the law is ingeniously adapted, sovereignty can be reasserted even beyond national borders, using treaty-based instruments, jurisdictional clauses, and operational guarantees. In parallel, the thesis demonstrates that Italy's reliance on third-country private entities leads to significant risks regarding service continuity as well as jurisdictional loss and strategic dependency. These risks are amplified by geopolitical asymmetries characterizing current transatlantic relations and the increasing politicization of infrastructure control by non-state actors.

The DDL Spazio introduces a strong, albeit incomplete, legal groundwork for national regulation of orbital and satellite services, its provisions on licensing, strategic control, and public-private collaboration are steps in the right direction. However, as argued throughout the thesis, there are currently no clear protections regarding data localization, jurisdictional enforceability, or extraterritorial resilience. Subsequently, the thesis has proposed the integration of models such as the one of data embassy in order to bridge these normative gaps. This comprehensive approach, which grounds sovereignty not solely in law but also on technical standards and geopolitical strategy, provides a viable path forward for Italy and other EU Member States facing similar challenges.

Importantly, this research also opens doors to several opportunities for future inquiry on the topic. As the geopolitical balance continues to shift, particularly with renewed infrastructural autonomy by the United States and China, there is an urgent need to examine how international alliances such as the EU and NATO can coordinate digital sovereignty

initiatives while not fragmenting global data governance. Likewise, the role of private entities like SpaceX in shaping not just technical infrastructures but also regulatory outcomes, should be studied more critically, especially in light of increasing personalization of executive power in transnational platforms.

Ultimately, this thesis has argued that sovereignty in the modern age can no longer be presumed: it must be designed, embedded and continuously renegotiated. By combining legal consistency with strategic forethought, the frameworks proposed here aim to prepare states like Italy with the tools necessary to remain autonomous, even in a world where infrastructure is global, borderless, and frequently beyond conventional political control.

# Bibliography


Agenzia per l'Italia Digitale (AGID), Linee guida sull'accessibilità degli strumenti informatici della PA (2024). Available at: https://www.agid.gov.it/sites/agid/files/2024-06/Linee%20Guida%20sull%27accessibilit%C3%A0%20degli%20strumenti%20informatici%20-%20PA.pdf.

Agenzia per la Cybersicurezza Nazionale (ACN), Strategia nazionale di cybersicurezza 2022–2026 (2022). Available at: https://www.acn.gov.it/portale/documents/20119/531899/ACN_Strategia.pdf/81644476-f547-6a63-dda6-3356f4d1b2f6?t=1719931791748.

Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems. Available at: https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf.

Amazon Web Services (AWS), New edge location in the Kingdom of Saudi Arabia (2025), AWS News. Available at: https://aws.amazon.com/it/about-aws/whats-new/2025/01/new-edge-location-kingdom-saudi-arabia/.

Amazon Web Services (AWS). (2019). AWS Middle East (Bahrain) Region Now Open: Expanding Cloud Services in the GCC. AWS Public Sector Blog. Available at: https://press.aboutamazon.com/2017/9/amazon-web-services-announces-the-opening-of-data-centers-in-the-middle-east-by-early-2019.

American Journal of International Law, (1985) THE ABUSE OF DIPLOMATIC PRIVILEGES AND IMMUNITIES: RECENT UNITED KINGDOM EXPERIENCE, Editorial Comment *641. Available at: https://www.ilsa.org/Jessup/Jessup07/basicmats/ajil_higgins_article.pdf.

Anna-Maria Kolessova. (2023). Estonia's Data Embassy Initiative: A Framework for Building Cyber Resilience in Other Countries. Tallin University of technology. Available at: https://digikogu.taltech.ee/et/Download/dae125ad-ef19-4f5b-b087-305bdfc2aed2.

APEC, Cross-Border Privacy Rules (CBPR) System Available at: https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf.

Ars Interpretandi (2024) Dossier: Spazio e Diritto – Profili normativi del nuovo scenario spaziale europeo, Ars Interpretandi, 2/2024. Available at: https://www.arsinterpretandi.it.

Bahrain eGovernment Portal. (n.d.). Bahrain's Digital Transformation and Cloud Strategy. Government of Bahrain. Available at: https://www.bahrain.bh/wps/portal/en/.

BBC News. (2020). India bans nearly 60 Chinese apps, including TikTok and WeChat, citing security concerns. Available at: https://www.bbc.com/news/world-asia-india-53226295.

Benvenisti, E. and Lustig, D., 2008. Reclaiming democracy: The strategic uses of foreign and international law by national courts. American Journal of International Law, 102, pp.241–274. https://doi.org/10.1017/S0002930000016704.

Binnendijk, A., Cohen, R.S., Frederick, B. and Geist, E., Mitigating Risks to the U.S. AI Innovation Ecosystem: Selective Decoupling and the AI Diffusion Strategy (2024), RAND Corporation. Available at: https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3700/PEA3776-1/RAND_PEA3776-1.pdf.

Bradshaw, S., Millard, C. and Walden, I., Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services (2011), International Journal of Law and Information Technology, 19(3), pp. 187–223. Available at: https://doi.org/10.1093/ijlit/eaq017.

Camera dei Deputati – Servizio Studi (2024) Elementi di valutazione del DDL "spazio" (AC 163). Available at: https://www.camera.it/temiap/documentazione/temi/pdf/1472496.pdf?_1747318974496.

Camp, L.J. (2000). Trust and Risk in Internet Commerce. Cambridge: MIT Press. Available at: ISBN: 9780262531979.

Catanzariti, M. (2024) Disconnecting Sovereignty: How Data Fragmentation Reshapes the Law, Springer. Available at: https://doi.org/10.1007/978-3-031-60734-9.

Court of Justice of the European Union. (2020). Case C-311/18: Data Protection Commissioner v. Facebook Ireland Ltd and Maximilian Schrems (Schrems II). Available at: https://curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=EN.

Cyber Defense Magazine (2024) Cybersecurity Threats in Global Satellite Internet. Available at: https://www.cyberdefensemagazine.com/cybersecurity-threats-in-global-satellite-internet/.

Deloitte. (2022) Digital sovereignty and economic growth: The role of secure data infrastructure. Available at: https://www2.deloitte.com/global/en/insights/industry/technology/digital-sovereignty.html.

DGA Group, Saudi Arabia introduces a draft Global AI Hub Law (2024). Available at: https://dgagroup.com/insight/saudi-arabia-introduces-a-draft-global-ai-hub-law/#:~:text=Overview%20of%20the%20law,consultation%20until%20May%2014%2C%202025.

European Commission, IRIS² – Secure Connectivity (n.d.). Available at: https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en.

European Commission. (2021). Digital Public Services and Interoperability: The Evolution of E-Government in the EU. Brussels: European Union Publications Office. Available at: https://digital-strategy.ec.europa.eu/en/library.

European Data Protection Board (EDPB). (2020). Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

European External Action Service (2025) EU–US Tensions Escalate Over Digital Tax and Tariff Disputes. EU Strategic Outlook Briefing No. 12. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1149.

European Union Agency for Cybersecurity, (2024). 2024 report on the state of cybersecurity in the Union: Condensed version. ENISA. Available at: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20Cybersecurity%20in%20the%20Union%20-%20Condensed%20version.pdf.

European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Articles 44–46, Official Journal of the European Union, L119, pp. 1–88. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

European Union. (2016). General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679. Official Journal of the European Union. Available at: https://gdpr.eu/.

Fernandez, M. (2023). Towards a New International Framework for Data Governance: Proposing Data Embassy Status for Global Data Centres. SSRN. Available at: http://dx.doi.org/10.2139/ssrn.4991958.

Floridi, L., (2021). The data economy: Understanding the value of data and the regulation of the data market. Journal of Information Policy, 11, pp.26–41. Available at: https://doi.org/10.5325/jinfopoli.11.2021.0026.

Forecast International (2024) Potential Use of Starlink by Russia: A Background and the Implications, Defense & Security Monitor. Available at: https://dsm.forecastinternational.com/2024/05/15/potential-use-of-starlink-by-russia-a-background-and-the-implications/.

France. Loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales. Paris: Journal Officiel de la République Française. Available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000018931380/.

Fruhwirth, M. (2023, July 17). Tackling foreign election interference through self-determination. Völkerrechtsblog. Available at: https://voelkerrechtsblog.org/tackling-foreign-election-interference-through-self-determination/.

GAIA-X European Association for Data and Cloud AISBL. (n.d.). What is GAIA-X? Available at: https://gaia-x.eu/.

Gartner. (2021) Strategic planning for cloud sovereignty: The future of data protection and business expansion. Available at: https://www.gartner.com/en/insights/cloud-sovereignty.

Google Cloud, Google Cloud expands regional presence with opening of Dammam cloud region, forecast to boost economy by USD 109 billion by 2030 (2023), Google Cloud Press Corner. Available at: https://www.googlecloudpresscorner.com/2023-11-15-Google-Cloud-Expands-Regional-Presence-with-Opening-of-Dammam-Cloud-Region-Forecast-to-Boost-Economy-by-USD-109-Billion-by-2030.

Hafner-Burton, E.M., Helfer, L.R. and Victor, D.G., 2009. Political science research on international law: The state of the field. The American Journal of International Law, 103(3), pp.291–324. Available at: https://doi.org/10.2307/20685861.

Heller, M. (2017). The Estonian Data Embassy Initiative: Protecting Digital Infrastructure from Modern Threats. Royal Holloway, University of London. Available at: https://pure.royalholloway.ac.uk/ws/portalfiles/portal/28736263/Network_Security_Article_Estonian_Data_Embassy_Initiative.pdf.

Immunities and Criminal Proceedings (Equatorial Guinea v. France), Judgment, I.C.J. Reports 2020, p. 300. Available at: https://www.icj-cij.org/case/163.

International Court of Justice (ICJ), 1980. United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment of 24 May 1980. ICJ Reports 1980, p. 3. Available at: https://www.icj-cij.org/en/case/64.

International Telecommunication Union (ITU). (n.d.). ITU cybersecurity work programme for developing countries. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

Isaac, M. and Sanger, D. E. (2023) Elon Musk's Starlink Decision Disrupted a Ukrainian Attack. The New York Times, 7 September. Available at: https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html.

Istituto Affari Internazionali (IAI) (2021) Space and European Digital Sovereignty: The Role of Italy. IAI Papers 21|11. Available at: https://www.iai.it/sites/default/files/iai2111_en.pdf.

Kuner, C., Transborder data flows and data privacy law (2014) Computer Law & Security Review, 30(1), pp. 104–108. Available at: https://doi.org/10.1016/j.clsr.2013.12.003.

Legifrance (2008) Loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales. Available at: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000018931380/.

LuxConnect. (2018). Tier IV Data Centers and Their Role in National Security Strategies. Luxembourg: LuxConnect. Available at: https://www.luxconnect.lu/.

Luxembourg Ministry of Digitalisation. (n.d.). Data Embassy Initiative. Available at: https://innovative-initiatives.public.lu/initiatives/data-embassy.

Mallett, M.E. & Hale, J.R. (2006). The Military Organization of a Renaissance State: Venice, c. 1400 to 1617. Cambridge: Cambridge University Press Accessed. Available at: https://doi.org/10.1017/CBO9780511562686.

McKenna, A. 2021 Myanmar coup d'état. Encyclopedia Britannica. Available at: https://www.britannica.com/event/2021-Myanmar-coup-d-etat.

MEAC (2016). Transforming digital continuity: Enhancing IT resilience through cloud computing, Ministry of Economic Affairs & Communications and Microsoft, Tallinn. Available at: https://www.digar.ee/viewer/en/nlib-digar:280707/252096/page/1.

Meritocrazia Italia (2024) D.D.L. Spazio: «Mi chiede misure volte a evitare che entità come SpaceX operino senza controlli adeguati». Available at: https://www.meritocrazia.eu/d-d-l-spazio-mi-chiede-misure-volte-a-evitare-che-entita-come-spacex-operino-senza-controlli-adeguati/.

Microsoft & Republic of Estonia. (2016). Implementation of the Virtual Data Embassy Solution: Summary Report. Microsoft Corporation. Available at: https://download.microsoft.com/download/5/5/B/55B89687-C789-43DE-A5B1-89D9CE6BCF71/Implementation%20of%20the%20Virtual%20Data%20Embassy%20Solution%20Summary%20Report.pdf.

National Competitiveness Center (NCC), Global AI Hub Law – Final Draft for Public Consultation (2024), Istitlaa Platform, available at: https://istitlaa.ncc.gov.sa/en/transportation/citc/globalailaw/Documents/Global%20AI%20Hub%20Law%20EN-AR%20-%20Final%20Draft%20for%20PC.pdf.

National People's Congress of China. (2017). Cybersecurity Law of the People's Republic of China. Available at: https://www.chinalawtranslate.com/en/cybersecurity-law-2016/.

NATO Strategic Communications Centre of Excellence (StratCom COE). (n.d.). Cyber Attacks Against Estonia 2007. Available at: https://stratcomcoe.org/pdfjs/?file=/publications/download/cyber_attacks_estonia.pdf?zoom=page-fit.

Obiene, F.M., 2024. Diplomatic law reimagined: Appraising the risks and prospects of data embassies. Law School Policy Review. Available at: https://lawschoolpolicyreview.com/2024/01/23/diplomatic-law-reimagined-appraising-the-risks-and-prospects-of-data-embassies/.

Pinsent Masons, Saudi Arabia strengthens data sovereignty through draft AI hub law (2024), Out-Law News. Available at: https://www.pinsentmasons.com/out-law/news/saudi-arabia-data-sovereignty-ai-hub-law.

Posner, R. A. (1972). Archives and the Public Interest: Selected Essays by Ernst Posner. Washington, D.C. Public Affairs Press. Available at: http://files.archivists.org/pubs/free/ArchivesInTheAncientWorld-2003.pdf.

R (on the application of Bancoult No 3) (Appellant) v Secretary of State for Foreign and Commonwealth Affairs (Respondent). Available at: https://supremecourt.uk/uploads/uksc_2015_0022_judgment_af89da8fbf.pdf.

Reuters. (2023). Huawei banned: Which countries have restricted the use of 5G kit? Available at: https://www.reuters.com/world/huawei-banned-which-countries-have-restricted-use-5g-kit-2023-08-10/.

Robinson, L., Kask, L. and Krimmer, R., 2019. The Estonian Data Embassy and the Applicability of the Vienna Convention: An Exploratory Analysis. In: Kerstin Martens et al. (eds.), Diplomacy in the Digital Age. University of Tartu. Available at: https://doi.org/10.1145/3326365.3326417.

Russian Federation. (2015). Federal Law on Personal Data and Data Localization Requirements. Available at: https://iapp.org/news/a/russias-data-localization-law-requirements-and-compliance/.

Sanger, D.E. and Kramer, A.E. (2024) Ukraine Confronts New Security Threat as Russia Gains Access to Starlink. The New York Times, 24 May. Available at: https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

Satariano, A., Saudi Arabia spends billions to build an A.I. industry from scratch (2024), The New York Times, 19 March. Available at: https://www.nytimes.com/2024/03/19/business/saudi-arabia-investment-artificial-intelligence.html.

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W.W. Norton & Company. Available at: ISBN: 978-0-393-35217-7.

Shear, M.D. and Conger, K. (2025) Trump Appoints Elon Musk to Lead New Federal Tech Office. The Washington Post, 2 February. Available at: https://www.washingtonpost.com/politics/2025/02/02/trump-musk-doge-appointment/.

Sierzputowski, B. (2019) 'THE DATA EMBASSY UNDER PUBLIC INTERNATIONAL LAW', International and Comparative Law Quarterly, 68(1), pp. 225–242. Available at: doi:10.1017/S0020589318000428.

Telespazio, Space Alliance: follow-on contract signed with the Italian Ministry of Defence for SICRAL 3 (2020). Available at: https://www.telespazio.com/it/news-and-stories-detail/-/detail/space-alliance-follow-on-contract-sicral3.

The White House. 2025. Fact Sheet: President Donald J. Trump Secures Historic $600 Billion Investment Commitment in Saudi Arabia. May 13. Available at: https://www.whitehouse.gov/fact-sheets/2025/05/fact-sheet-president-donald-j-trump-secures-historic-600-billion-investment-commitment-in-saudi-arabia/.

U.S. Congress. (2018). Clarifying Lawful Overseas Use of Data (CLOUD) Act. Available at: https://www.congress.gov/bill/115th-congress/house-bill/4943.

U.S. Department of Commerce, Framework for Artificial Intelligence Diffusion, Federal Register, Vol. 90, No. 10 (15 January 2025), Document No. 2025-00636. Available at: https://www.federalregister.gov/documents/2025/01/15/2025-00636/framework-for-artificial-intelligence-diffusion.

United Nations E-Government Survey. (2022). Estonia: A Model for Digital Governance. New York: UN Department of Economic and Social Affairs. Available at: https://publicadministration.un.org/egovkb/.

United Nations, 1961. Vienna Convention on Diplomatic Relations. 500 UNTS 95. Available at: https://legal.un.org/ilc/texts/instruments/english/conventions/9_1_1961.pdf.

Ward, I., 1977. Espionage and the forfeiture of diplomatic privileges. Journal of International Law and Policy, 5(3), pp.221–242. Available at. https://scholar.smu.edu/til/vol11/iss4/6.

Wikipedia (2024) Starlink in the Russian-Ukrainian War. Available at: https://en.wikipedia.org/wiki/Starlink_in_the_Russian-Ukrainian_War.

World Economic Forum. (2021) The geopolitics of data: Why sovereignty matters. Available at: https://www.weforum.org/reports/the-geopolitics-of-data.