ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 3, March 2026

Data Embassies: Reimagining Sovereignty and Its Future in the Digital Age

[1] Kiran Bisht, [2] Dr. Niru Sharan

[1] Amity Institute of International Studies, Noida, Uttar Pradesh, India
[2] Amity Law School, Noida, Uttar Pradesh, India
Corresponding Author Email: [1] kiranb2899@gmail.com, [2] nsharan@amity.edu

Abstract*— The emergence of the data embassy marked a significant new dimension of state sovereignty in the digital age, where governments are increasingly dependent on digital infrastructure. To examine how states ensure continuity, resilience and authority over important digital assets in an era of cyber threats, geopolitical uncertainty and systemic risks to national data. This study demonstrates the data embassy as a strategic mechanism for ensuring uninterrupted digital continuity, with specific emphasis on the Estonia-Luxembourg models as its central case. The paper also provides a brief overview of the data center and its growing relevance in the digital age for the smooth conduct of government and further explores the rationale behind the establishment of the data embassies, outlining the conceptual foundations, institutional design and governance structure. The paper takes a comparative approach to assess the unique approaches of Luxembourg and Bahrain, and it also delves into the new initiatives in India and Saudi Arabia. The study also examines the new ways of shared and networked sovereignty, where the host and guest nations work together to oversee the data embassy with different legal systems. The paper concludes that data embassies represent a new frontier in digital diplomacy and sovereignty. But for data embassies to work, there is a need for international legal frameworks, secure infrastructure and mutual trust between the host and guest countries.

Index Terms*— Data Centre, Data Embassy, Digital Sovereignty, International Relations, Vienna Convention on Diplomatic Relations (VCDR).

I. INTRODUCTION

Data embassy: the concept first emerged in 2017, when Estonia established its first data embassy in Luxembourg to back up its national data. This initiative extended the traditional logic of diplomatic infrastructure into the digital domain. Traditionally, embassies have long served as a physical infrastructure or a sovereign space abroad that provides protection, assistance and legal recognition to their citizen residing or travelling overseas. However, we are now seeing a new concept in an embassy that differs from the traditional embassy: the data embassy, an innovative solution in the era of digitalization. The advent of the internet brought challenges like cyber threats, data breaches, and digital interdependence, which led to the protection of national data becoming a core element of state security. A data embassy showcases the new form of model that is digital sovereignty, where a nation stores its critical data on state-owned servers located outside its territory, usually within trusted foreign 'Data Centers'. These facilities, functioning as secure "digital embassies," make sure that government operations can continue even during crises such as cyberattacks, wars, or natural disasters. According to the Data Security Council of India, "Digital Embassy is an extension of a nation's cloud computing infrastructure using government-owned servers in a foreign land" (TOI Tech Desk, 2026).

II. UNDERSTANDING THE CONCEPT OF DATA CENTRE

To understand the concept of data embassy, it is important to have a better understanding of what a data center is. According to Amazon Web Services, a data center is a dedicated facility that is designed to store computing and networking infrastructure, including servers, storage devices, and communication systems. The facility is centralized for managing, storing, processing, and distributing large volumes of digital data. The capacity of the data center ranges from a small room to a vast industrial complex that houses vital IT infrastructure critical for business, governments, or cloud computing operations (Amazon Web Services, 2025). To operate smoothly, a data center requires a robust support system, which is crucial for ensuring reliability, reducing service interruptions, ensuring continuous service availability, and protecting data integrity. The key components of this support infrastructure are, first, a reliable power supply, often accompanied by Uninterruptible Power Supply (UPS) units to provide emergency power during electrical outages. Second, a cooling system helps in regulating temperature and humidity to prevent overheating. Third, fire detection and suppression. Fourth, physical security, such as fencing, surveillance cameras, security guards, and biometric control. Fifth, network infrastructure, high-speed connections, routers, switches, and firewall protection are necessary to maintain data flow and network security. Sixth, environment monitoring is crucial to detect

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 3, March 2026

and prevent hazards by using sensors to monitor temperature, humidity, smoke, water leaks, and power consumption. Last, structural and architectural design, meaning building with earthquake resistance, flood prevention, and secure construction.

Data centers can be distinguished by several factors such as ownership, technological specifications, storage capacity, and energy efficiency. However, the four primary categories of data centers are as follows. First, the Enterprise Data Centre, these are in-house facilities constructed, owned, and operated by companies, optimized to serve their end-users. Such centers have greater control over their information (Flexential, 2023). Second, Managed Services Data Centers involve companies leasing equipment and infrastructure rather than purchasing them, with the data centers being managed by a third-party service provider on behalf of the company. Third, Colocation Data Centers, here, a company rents space within a data center owned by an external entity and located off its premises. The colocation center provides the necessary infrastructure, including building, cooling, bandwidth, and security; however, the company supplies and manages the essential components such as servers, storage solutions, and firewalls. Last, Cloud Data Centers are off-premises facilities where data and applications are hosted by cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, IBM Cloud, or other public cloud providers (Cisco, 2025). These factors are critical for a nation in assessing and determining the categories of services for which it intends to host data within the jurisdiction of a partner nation.

III. DATA CENTRE INFRASTRUCTURE AND STANDARDS

Establishing standardized norms for data center infrastructure and operational practices is essential. The Uptime Institute, a global authority that sets standards and provides consulting services for the construction and operation of data centers, has standardized the data center data organization into four tiers. Tier 4 is the most advanced and fault-tolerant, while Tier 1 has the least sophisticated infrastructure (Bilal Khan, 2024). In a Tier 1 data center, there is limited protection against physical events. It has single-capacity components and a single, nonredundant distribution path (Cisco, 2025). Regarding redundancy, there is power, cooling, and network redundancy, which ensures smooth data center. operation. Tier 2 offers improved protection against physical events. It includes redundant components such as cooling systems and power supplies. Tier 3 has multiple power and cooling pathways, as well as options to update and repair without system shutdown. Tier 4 is fully fault-tolerant with completely redundant systems and can continue operating even during severe failures. Estonia chose a Tier 4 facility in Luxembourg, which is the highest level of data facility (e-Estonia, 2025). The cost of a standard data center ranges from approximately $7 million to $12 million. The cost may vary according to location, and specific operational need (reliable power supply, backup generators, cooling system and high-speed connectivity) (Marx, G., 2025). The standard development of standardized data centers strengthens trust and credibility between the nations, while cost- efficient operation with comprehensive facilities makes such infrastructures a preferred choice for countries seeking cross-border data hosting arrangements.

IV. DATA EMBASSIES: CONCEPT AND GOVERNANCE

Conceptualizing the basic idea of data embassy, it is necessary to examine what it entails and how it is distinct from, yet interchangeably used with, the term ‘digital embassy’. While a digital embassy represents a broader framework encompassing multiple aspects of digital diplomacy and virtual state presence, this discussion is confined specifically to the concept of a data embassy, which focuses on the storage, protection, and governance of data. In this sense data embassy is a critical component of the state's digital infrastructure, particularly when there are growing cyber threats and geopolitical uncertainty.

A data embassy is a vital infrastructure that requires a secure and resilient data system capable of protecting a nation’s data from both cyber and physical threats (armed conflict and natural disasters). Beyond security, the system should have an effective mechanism to ensure efficient data back-up to ensure operational continuity in a crisis. Central to the functioning of the data embassy is the presence of a trusted partner that covers technical and contractual measures to ensure the confidentiality, integrity and availability of the data stored within the facility (Thiebaut Meyer, 2022).

While data center infrastructure continues to form the backbone of data storage, cloud technology has emerged as an evolving concept that enables governments to leverage globally distributed infrastructure and store their data across vast geographic locations. However, the reliance on external infrastructure also necessitates clearly defined governance mechanisms between the home and host countries. In this context, it's also important for the host and home country to establish the three pillars of sovereignty on the recovery site. First is the Data Sovereignty, which is important for the home country to have access and control over its data, which is protected and not subject to the host country’s jurisdiction. This can be achieved when the nation has the encryption keys to unlock the data. The Second pillar, Operational Sovereignty, requires that the home country have continuous visibility and control over the provider operations even during extreme scenarios (Thiebaut Meyer, 2022). The third pillar is Software Sovereignty, the home country can choose the technical stack without depending on the providers (Thiébaut Meyer, 2022). Together, these pillars are crucial for the effective development and functioning of a data

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 3, March 2026

embassy. It contributes significantly to trust building between the nations and reinforces the broader objective of digital sovereignty and secure cross-border data governance.

V. WHY IS THERE A NEED FOR A DATA EMBASSY?

The need to establish the data embassy arises from the nature of conflict that is evolving. We are living in a new era of conflict that is hybrid in nature and crosses boundaries that were hitherto known, including cyberspace and targets government databases. Data embassy ensures the continuity of government digital services, even when governing from within a country's borders becomes unfeasible during crises such as armed conflict or natural disasters. A prime example is Estonia; it is the most digitized country that faced a cyberattack lasting 22 days from April 27 to May 18, 2007. It paralyzed many entities, including the government, the president, the parliament, the police, banks, Internet service providers (ISPs), online media, as well as many small businesses and local government sites (Ottis, 2008). Following this, the Estonian government took significant steps to enhance its cybersecurity. On 20 June 2017, Estonia became the first country in the world to establish a Data Embassy when Prime Minister Jüri Ratas and Luxembourg's Prime Minister Xavier Bettel signed a bilateral agreement to host Estonia's critical digital assets in Luxembourg. Successive Estonia's story, other countries have also adopted the model; for instance, Monaco inaugurated its own data embassy in Luxembourg in 2021, and meanwhile, Bahrain issued a legislative decree that created a legal framework for data stored in Bahraini data centers (Thiébaut Meyer, 2022). These cases highlight how nations are re-evaluating sovereignty in cyberspace and developing legal methods for cross-border data storage.

VI. LUXEMBOURG AND BAHRAIN: A COMPARATIVE PERSPECTIVE

Luxembourg's approach to the data embassy concept is embodied in a state-to-state model. The bilateral agreement between Estonia and Luxembourg, as well as considering the Vienna Convention on Diplomatic Relations (VCDR), has led to the establishment of a government-operated data center in Betzdorf for hosting Estonian data. The arrangement is overseen by the competent authorities, namely the Ministry of Economic Affairs and Communications for the Republic of Estonia, and the "CTIE (Centre des technologies de l'information de l'État - The State Information Technology Centre)" for the Grand Duchy of Luxembourg (The Republic of Estonia & The Grand Duchy of Luxembourg, 2017). Access to the facility by Luxembourg officials is strictly controlled; they can only enter the facility with Estonia's authorization, except in emergency situations. The data center is protected from search, requisition, and legal enforcement. The data stored there is considered as Estonian archives, and communications are secured similarly to those of diplomatic missions, using encryption and diplomatic messengers. This framework for data management is governed by international and EU law, with any disputes being resolved by a three-member arbitral tribunal. Furthermore, either party can end the agreement with a 24-month notice period, ensuring that the protection for Estonia's assets is continued after termination. Since 2018, an extension of the Estonian Government's 'cloud' has been hosted at LuxConnect's certified Tier IV data center (Government of the Grand Duchy of Luxembourg, 2025). LuxConnect, a government-funded yet privately operated data center and networking company, manages several facilities ranging from Tier II to Tier IV in Bettembourg and Bissen (Dawn-Hiscox, 2017). After the success of the Estonian data embassy in Luxembourg, the second country to establish a digital embassy was Monaco, which launched its data embassy in September 2021.

The success of Luxembourg in this regard can be attributed to two major factors: first, its outstanding telecommunications infrastructure. As stated in the Digital Economy and Society Index 2020, Luxembourg is ranked 3rd in Europe regarding connectivity. Second, the country has vast experience in the field of cybersecurity.

Bahrain, a small state in the Middle East, has established the Legislative Decree Number 56 of 2018, which offers cloud computing services to third-party countries. This legislation creates a framework that enables third-party countries to invest in cloud computing services offered in Data Centers. The act clearly states that the data held by third-party consumers is subject to the laws of their country of residence, and the courts of the foreign country have jurisdiction over any legal matters about the data.

Luxembourg and Bahrain are the two nations that have set up the data centers, but there is a huge contrast between them. If we look at the Luxembourg model, they established a government-to-government agreement to ensure the nation's digital continuity. It involves a sovereign state establishing a physical presence of a set of servers in a government-owned data center, and the data and servers themselves are granted diplomatic immunity, similar to a traditional embassy, meaning they are inviolable and under the jurisdiction of the partner country. In the Bahrain model, it is less about government-to-government agreement and more about creating a favorable legal environment for all types of data storage. It gives a legal framework to attract foreign investment in its cloud computing sector. It establishes a jurisdictional framework rather than a physically sovereign one with diplomatic immunity like Luxembourg (Fawcett, Jhala, & Osman, 2020).

VII. EMERGING DATA EMBASSY INITIATIVES

India - For the first time in the budget speech on February 1 2023, Indian Finance Minister Smt. Nirmala Sitharaman

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Volume 13, Issue 3, March 2026

stated that the Indian government would advance the establishment of data embassies for countries to look for a digital continuity solution (Barat D, 2023). In her speech, the finance minister announced that the government would assist in setting up a data embassy in the Gujarat International Finance Tec-city (GIFT) in India's first International Finance Service Centre (IFSC) (Barat D, 2023). According to Business Line 2025, Singapore is actively considering GIFT City in Gujarat as a location for setting up the Data Embassy, as stated by Dipesh Shah, Executive Director, Department of Development, International Financial Centers Authority (IFSCA). The Central Government, in its interim budget announcement in 2024, stated that the establishment of data embassies in GIFT IFSC will primarily be facilitated in the form of bilateral agreements between India and the interested countries (The Hindu Business Line, 2025).

Saudi Arabia - On April 14, 2025, Saudi Arabia's Communication, Space Technology Commission (CST) introduced the first draft of the Global AI Hub Law (Meenagh, Koroleva, & Imam, 2025). They defined three categories of AI Hub. First Private Hub, in this, the guest country can operate under the bilateral agreement with Saudi Arabia, under the laws and regulations of the guest country. Second, Extended Hub here, the third party can operate under an agreement with the competent authority and according to the guest country's laws and regulations. Last is Virtual Hub, in this, a third-party operates as a service provider operating in Saudi Arabia and approved by the competent authority to offer a virtual hub for use by customers of the service provider according to the laws and regulations of a "Designated Foreign State" (Meenagh, Koroleva, & Imam, 2025). The CST clearly distinguished the rules for foreign government (Private Hubs), foreign company (Extended Hubs), and data center providers who want to comply with foreign government laws while hosting data in Saudi Arabia (Virtual Hub) (Meenagh, Koroleva, & Imam, 2025).

VIII. LEGAL AND THEORETICAL FRAMEWORK

Vienna Convention Principles—largely inspired by the Vienna Convention on Diplomatic Relations 1961 (VCDR), which establishes that the premises, archives, and communications of a diplomatic mission are inviolable and exempt from search or legal processes by the host country. Articles 22 and 24 of the VCDR specify that the host state must protect embassy premises and grant immunity to diplomatic archives, including electronic records. Bilateral Treaties, as in the Estonia-Luxembourg treaty, clearly provide that the data embassy is under the sole jurisdiction of Estonia, thus ensuring that the Grand Duchy of Luxembourg cannot access or tamper with the data without the consent of Estonia. National Legislation, as in Bahrain and Saudi Arabia, has implemented national laws that provide that data stored in data embassies is under the jurisdiction of the countries of origin and not subject to local laws, thus encouraging foreign investment in the digital sector while ensuring data sovereignty.

Theoretically, the data embassy represents an alternative and new definition of the Westphalian concept of sovereignty, which is founded on the idea of the exclusive territorial principle of sovereignty. In the 21st century, the boundaries are no longer geographical; instead, sovereignty is increasingly exercised in cyberspace. As a result, the concept of sovereignty has changed, and new concepts of sovereignty have been developed, including digital sovereignty, shared sovereignty, and networked sovereignty, which correspond to the changing relationship between states, technology, and governance.

The data embassy is a concept of shared sovereignty where the sovereignty of the guest country and the host country is shared in the governance of the data embassy. It can also be referred to as a partnership. According to Stephen D Krasner, shared sovereignty is the involvement of external actors in some of the domestic governance structures of the target state for an indefinite period of time, and agreements signed by officially recognized authorities are what legitimize such structures. In the context of the agreement between Estonia (Guest Country) and Luxembourg (Host Country), both have their own roles: the host country offers infrastructure, security, power, and network connectivity, while the guest country is responsible for the legal jurisdiction of the data and access. This is a hybrid model where sovereignty is not absolute but shared through agreements. In this regard, it is also important to draw a distinction between digital sovereignty and data sovereignty, which are two concepts that deal with two different issues related to control in the digital environment. Data sovereignty concerns the legal authority over data, based on its storage location or ownership of the underlying infrastructure. In contrast, Digital sovereignty includes a broader scope; it refers to control over digital infrastructure, cloud platforms, software systems, standards, and governance. In the context of a data embassy, the data is hosted in another country but remains under the legal and political control of the sending state. The European Union exemplifies this principle through the General Data Protection Regulation (GDPR). According to this, any organization must comply with data management laws if it wants to do business with customers in EU countries.

Extending further, the rise of networked sovereignty- the internet has enabled a new network structure that operates in a decentralized way and bypasses the traditional power structures (Couldry 2015). The concept of network sovereignties is to describe the emergence of self-sovereign networked political communities that operate as an engine for global coordination, transcending the definition of traditional sovereignty (De Filippi et al. 2023). They do not replicate the state-centric model of sovereignty, nor do they seek to replace the institution of the state (Global Governance Programme, 2025). Instead, they exist in parallel with

existing state formation and work in coordination and cooperation in an interconnected world (Pohle & Thiel, 2020).

In this sense, the data embassy can be viewed as a combination of networked and shared sovereignty operating in parallel yet grounded in traditional diplomatic principles.

IX. CONCLUSION

The data embassy represents more than a technical solution; it personifies a redesign of diplomacy and statecraft in the information age. It gives nations a way to ensure digital continuity, sovereignty, and the security of digital assets in an ever-more unpredictable cyberspace. On the other hand, the current models, such as the ones in Luxembourg and Bahrain, demonstrate a different approach, whether it is diplomatic or legislative, and both demonstrate the increasing awareness of data as a sovereign state. However, there are still some challenges that exist. But some things need to be taken into consideration first: the location of the host nation—if the nation is in a conflict area, then the data center will always be a target. Second, the host nation needs to have enough resources to manage the data centers. Therefore, the selection of the host nation needs to take into consideration its political stability, security, and resources. There is also a need for international laws to ensure there are no misunderstandings about jurisdiction**.**

REFERENCES

[1] Cisco. What is a data center? 2025. https://www.cisco.com/c/en_ca/solutions/data-center-virtualization/what-is-a-data-center.html#~types-of-data-centers

[2] Meyer, Thiébaut. “Data Embassies: Strengthening Resiliency with Sovereignty.” Google Cloud Blog, November 12, 2022. https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty

[3] Government of Luxembourg. E-embassies in Luxembourg. 2025. https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html

[4] Dawn-Hiscox, T. Estonia to create “Data Embassy” in Luxembourg. 5 July 2017. https://www.datacenterdynamics.com/en/news/estonia-to-create-data-embassy-in-luxembourg/

[5] Khan, G. Data embassies in India. 24 October 2021. https://www.snrlaw.in/data-embassies-in-india/

[6] Fawcett, A., Jhala, K., & Osman, H. Diplomatic immunity for data: Bahrain’s Data Embassy Law. 29 March 2020. https://www.tamimi.com/law-update-articles/diplomatic-immunity-for-data-bahrains-data-embassy-law/

[7] Republic of Estonia. Agreement between the Government of the Republic of Estonia and the Government of the Grand Duchy of Luxembourg concerning the data embassy. 19 February 2018. https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf

[8] Sultan, A. Data embassies: Protecting nations in the cloud. 23 March 2021. https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/

[9] Barat, D. Data Embassies in India. 31 July 2023. https://www.snrlaw.in/data-embassies-in-india/

[10] The Hindu BusinessLine. Singapore “actively looking” to set up data embassy in GIFT City: IFSCA official. 14 February 2025. https://www.thehindubusinessline.com/news/national/singapore-actively-looking-to-set-up-data-embassy-in-gift-city-ifsca-official/article69201626.ece

[11] Khan, B. Data Center Tiers: What Are They & Why Do They Matter? 22 April 2024. https://www.servercolocation.uk/blogs/articles/data-center-tiers-what-are-they-why-do-they-matter?srsltid=AfmBOop5Ruv4NwqEe2ue45lTboaY0cCyABZXPN0Vqqh9u9KG45Cto1Ba

[12] Meenagh, B., Koroleva, K., & Imam, F. Saudi Arabia pioneers data embassies with publication of draft Global AI Hub Law. 14 April 2025. https://www.globalprivacyblog.com/2025/04/saudi-arabia-pioneers-data-embassies-with-publication-of-draft-global-ai-hub-law/

[13] Krasner, S. D. Sharing Sovereignty: New Institutions for Collapsed and Failing States. 2004. http://www.jstor.org/stable/4137587

[14] Global Governance Programme. Introduction: New Network Sovereignties: The rise of non-territorial states? 2025. https://globalgovernanceprogramme.eui.eu/project/new-network-sovereignties-the-rise-of-non-territorial-states/introduction-new-network-sovereignties/

[15] Amazon Web Services. What is a data center? 2025. https://aws.amazon.com/what-is/data-center/

[16] Ottis, R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. 2008. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

[17] e-Estonia. Data Embassy. 2025. https://e-estonia.com/solutions/e-governance/data-embassy/

[18] Flexential. What is a data center and why is it important for business? 9 May 2023. https://www.flexential.com/resources/blog/what-is-data-center

[19] Republic of Estonia & The Grand Duchy of Luxembourg. Agreement on the Hosting of Data and Information Systems (Luxembourg-Info Agreement). 20 June 2017. https://complexdiscovery.com/wp-content/uploads/2022/02/Luxembourg-Info-Agreement.pdf

[20] Minister of State, Government of the Grand Duchy of Luxembourg. E-embassies in Luxembourg. 2025. https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html

[21] Couldry, N. (2015). The myth of ‘us’: digital networks, political change and the production of collectivity. Information, Communication & Society, 18(6), 608-626.

[22] De Filippi, P., Schingler, J. K., de Kerhuelvez, L., Cossar, S., Mannan, M. (2023) “Network Sovereignties as a Mechanism for Global Coordination,” in Max Weber Programme Multidisciplinary Research Workshop ‘From Global to Local and Back: Untangling Glocal Governance.’ European University Institute. June 22, 2023

[23] Pohle, J., & Thiel, T. (2020). Digital sovereignty. Pohle, J. & Thiel.

[24] Marx, G. (2025, June 26). Cost of a data center. BlueCape Economic Advisors. Retrieved from https://www.bluecapeconomicadvisors.com/post/cost-of-a-data-center

[25] TOI Tech Desk. (2026, January 21). Understanding Digital Embassies: How India and UAE are exploring secure data hubs, AI collaboration, and global digital infrastructure. The Times of India. Retrieved from https://timesofindia.

indiatimes.com/technology/tech-news/understanding-digital-embassies-how-india-and-uae-are-exploring-secure-data-hubs-ai-collaboration-and-global-digital-infrastructure/articleshow/126792450.cms