Beyond Borders: Exploring Data Embassies as a Strategy for Digital Sovereignty in Africa

Authors

Samuel F. Matinou,[a] Isobel Acquah,[b] Ridwan Oloyede,[c] Arnold J. Kabatsi,[d] Prasenjit Mitra,[e] Conrad S. Tucker,[f]

Corresponding Author

Samuel F. Matinou
59 Avenue Jeanne
Chénnevière-Sur-Marne
Tel: + (353) 89 445 3608
Email: fmatinou@certafoundation.rw

[a] Samuel F. Matinou, European Master's in Law, Data and AI, (Erasmus Mundus Scholar); Research Affiliate at the Law and Tech Lab, Center for Law and Innovation, Certa Foundation.
[b] Isobel Acquah is the Africa Director of Certa Foundation in Rwanda.
[c] Ridwan Oloyede is the Director of the Center for Law and Innovation in Rwanda.
[d] Arnold J. Kabatsi is an Associate at the Center for Law and Innovation
[e] Prasenjit Mitra, Ph.D., is a Research Professor in the Department of Electrical and Computer Engineering at Carnegie Mellon University Africa and an Affiliate Research Professor at the Human-Computer Interaction Institute.
[f] Conrad S. Tucker is Director of CMU-Africa and Trustee Professor of Mechanical Engineering at Carnegie Mellon University, with courtesy appointments in Machine Learning, the Robotics Institute, and Biomedical Engineering.

Email: info@certafoundation.rw

Abstract

Data sovereignty, understood as the ability to maintain control over data as a strategic asset (Sciences Po, 2024), presents a complex challenge in Africa. This challenge is shaped by fragmented data protection laws, limited cross-border data transfer frameworks, and significant infrastructural deficits (African Leadership Magazine, 2024), all of which hinder the continent's ability to assert meaningful digital sovereignty. While over 40 African countries have enacted data protection laws, inconsistent implementation, insufficient operationalisation of transfer mechanisms still persist (Access Now, 2024). Again, over 10 countries still lack data protection legislation, resulting in a disaggregated landscape, particularly for personal data (Prinsloo & Kaliisa, 2022). Non-personal data on the other side remains largely unregulated across the African continent, with more than 60% of countries lacking any comprehensive data governance framework (Prinsloo & Kaliisa, 2022). Moreover, persistent infrastructural limitations, particularly unreliable power and limited secure hosting facilities, render localised data storage difficult to implement at scale (Banya, 2025). These interlinked legal and technical barriers not only weaken domestic control over data but also undermine trust in digital systems and limit cross-border cooperation on data sharing, digital trade, cybersecurity coordination, and regulatory harmonisation.

Against this backdrop, the concept of data embassies, as implemented in Estonia and explored in countries including Bahrain and India, offers a potential pathway. The premise of data embassies rests on the principle of embassy inviolability as outlined in the Vienna Convention on Diplomatic Relations (VCDR). The Convention enshrines the purposes and principles of the Charter of the United Nations concerning the sovereign equality of States, and advances the establishment of diplomatic relations and diplomatic missions, which are prone to a number of challenges, including the risk of political instability, unilateral interference, and breach of legal protections in the face of perceived national security by a host country. This position paper explores the potential of data embassies as a partial solution to Africa's digital sovereignty challenge. Using a comparative legal and policy analysis, it examines the Estonian model and assesses its applicability within Africa's legal, infrastructural, and political contexts.

The paper concludes by outlining key legal, institutional, and diplomatic considerations necessary for piloting such models in African settings, while proposing next steps for regional collaboration on sovereign digital infrastructure.

Keywords: *Data sovereignty and governance, Digital Infrastructure and Sovereignty, Data embassies, Data Centers, Vienna Convention on Diplomatic Relations*

I. Introduction

As data becomes increasingly important, central to most national security, economic resilience and social development, the notion of "data embassies" has emerged as a novel tool for safeguarding digital assets beyond physical borders. Among the various interpretations and standards found in academic and policy discourse, a particularly useful and actionable definition is: data embassies are data centres located in foreign jurisdictions, but under the full legal sovereignty of the originating country, secured through binding international agreements [1]. This concept distinguishes itself from other, more general interpretations that simply equate data embassies with off-site cloud backups or data localisation strategies [2].

Estonia, a pioneer in digital governance, operationalised the world's first data embassy in Luxembourg in 2017 [3], following a cyberattack in 2007 that exposed vulnerabilities in its digital infrastructure. While traditional data centers abroad may rely on standard service-level agreements (SLAs) and commercial cloud contracts, data embassies, as conceptualised by Estonia, are grounded in bilateral or multilateral diplomatic treaties [4]. These treaties ensure that host countries recognise the extraterritorial status of the data center, analogous to a physical embassy [5].

For the purposes of this position paper, we adopt the Estonian interpretation of data embassies, which is characterised by the assertion of legal extraterritoriality over data stored in foreign data centres in the host country instead of relying on the physical infrastructure of traditional embassies; digital sovereignty to ensure that data remains fully under the jurisdiction of the home state; strategic bilateral agreements to ensure diplomatic protection of the data center (in this case with Luxembourg); and secure, resilient continuity mechanisms, essential for critical digital government services.

While there is growing momentum across Africa to pursue digital sovereignty by asserting national control over digital infrastructure and citizen-generated data, the real challenge lies not only in securing legal authority over this data, but in sustaining the technical and financial capacity to store and manage it domestically [6]. In this paper, the focus shifts from concerns over data protection to the internal dimension of digital sovereignty:

How can African states ensure that data produced within their borders is governed by domestic laws, particularly when local digital infrastructure is inadequate?

Estonia's approach may offer a compelling case study for African nations seeking to build digital sovereignty without the immediate infrastructure for fully localised data centers. If supported by a harmonised legal framework across the African continent, these facilities could provide a shared infrastructure model, enabling countries to maintain legal jurisdiction over their data while avoiding the cost and complexity of unilateral infrastructural investment in the short to medium term.

In this sense, African digital sovereignty must be re-imagined not as a rigid insistence on territorial localisation, but as a strategic fusion of legal control, infrastructural pragmatism, and regional cooperation [7]. The future lies in building a continental data governance ecosystem based on mutual trust, aligned laws, and shared facilities, one where data embassies become a practical mechanism for upholding national autonomy in a digitally interdependent age.

Against this backdrop, the central question this paper poses is whether the Estonian approach to data embassies can be adopted or adapted by African countries to achieve meaningful digital sovereignty through the data embassy concept?

II. Estonian Data Embassy Model: Applicability of the VCDR Principles and the role of Bilateral Agreements

The agreement entered into between the Republic of Estonia and the Grand Duchy of Luxembourg provides for the hosting of Estonian data and information systems in Luxembourg. The agreement grants Estonia the right to use a dedicated section of a Luxembourg government-operated data center space, which is defined as the "premises" for the purpose of the agreement [8]. This arrangement was specifically created to ensure that Estonia could mirror and protect critical state data abroad in a manner consistent with the legal and operational protections normally afforded to diplomatic missions.

While the language of the agreement draws heavily on the structure and spirit of the VCDR (1961), creating a new class of international cooperation, it does not strictly rely on it. The agreement reflects the acknowledgment by both parties that the Convention alone was insufficient to fully govern such a novel arrangement.

In the absence of clear international precedent, the agreement functions as a reinterpretation and extension of diplomatic law into the digital domain. Estonian officials, recognising the legal uncertainties surrounding the application of the VCDR to data and digital infrastructure, opted not to refer to the arrangement as a "data embassy" within the text of the agreement. Instead, the agreement adopts a hybrid legal model, one that emulates key diplomatic protections while tailoring them to the specific needs of sovereign digital infrastructure [9].

With this legal context in mind, the core legal principles supporting the data embassy concept are the inviolability of diplomatic premises (Article 22 VCDR) and the inviolability of archives and documents (Article 24 VCDR) [10].

On the other hand, article 41(3) of the VCDR provides that the premises of a diplomatic mission must not be used in any manner incompatible with the functions of the mission, as outlined in the Convention or in general international law. This provision reinforces the principle that diplomatic premises must serve legitimate state functions [11]. In the context of data embassies, it opens the door for carefully crafted legal innovation, allowing the functional scope of diplomatic premises to evolve in line with contemporary state needs, such as the protection and continuity of critical digital infrastructure.

Through deliberate treaty-making and diplomatic coordination, the spirit of diplomatic inviolability can thus be extended to digital assets, provided such use remains consistent with sovereign functions recognised under international law [12].

The Estonia–Luxembourg Agreement reflects this logic in practice. It guarantees Estonia the right to conduct official communications and transmit documents within the host territory, consistent with the privileges afforded to traditional diplomatic missions.

Additionally, Luxembourg assumes a duty to protect the designated premises against intrusion or damage, ensuring a level of security equivalent to that which Estonia provides to Luxembourg's own diplomatic missions, an excellent demonstration of the principle of reciprocity in diplomatic law [13].

This reciprocal obligation establishes a "trust corridor": a space of mutual legal and political assurance that facilitates secure digital cooperation across borders, particularly when sovereign data is hosted extraterritorially under treaty-based protections.

Importantly, the agreement also includes provisions on dispute resolution. It specifies that any disagreement arising from the interpretation or application of the treaty, if not resolved through negotiation or mutually agreed means, shall be referred to a three-member arbitral tribunal established on a case-by-case basis [14]. This clause showcases the seriousness with which both parties regard the legal enforceability of the arrangement and reflects a growing international trend toward formalising digital sovereignty through binding dispute settlement mechanisms.

Crucially, the concept of "data embassy" is not explicitly visible in either the bilateral agreement or in the VCDR itself. Rather, it emerges from the interpretation of Article 22(1) and 24 of the VCDR. This invisibility, while creating some uncertainty, also offers strategic flexibility, particularly for regions such as Africa. In a context marked by infrastructural disparities, uneven treaty implementation, and evolving digital governance frameworks, this ambiguity allows room to reframe and adapt the model in ways that align with local realities and regional ambitions. It opens up space for African-led innovation in digital sovereignty, where bilateral or regional arrangements could draw from the Estonian model without being bound by its legal or infrastructural preconditions.

III. Africa's Pursuit of Digital Sovereignty

The rise of data-intensive technologies, such as artificial intelligence (AI) and the Internet of Things (IoT) in the Fourth Industrial Revolution (4IR), presents Africa with an unprecedented opportunity to leapfrog traditional developmental stages and forge new pathways to inclusive and sustainable growth. AI is a core technology within the 4IR, augmenting the transformative potential of these emerging technologies by enabling automation and promoting intelligent decision-making across industries and sectors. "AI is a strategic asset pivotal to achieving the aspirations of Agenda 2063 and the Sustainable Development Goals" and promises to ignite new industries, fuel innovation, and create high-value jobs while preserving and advancing African culture and integration [15].

As Africa leverages these emerging technologies and digitises its economies, governance systems, and public services, digital sovereignty becomes increasingly important due to the global nature of data flows and the ensuing potential risks, particularly those linked to data privacy and security. In principle, digital sovereignty refers to a nation's right to ensure that data generated by its citizens and within its borders is subject to its own legal frameworks, policy priorities, and constitutional values, as well as the right to exercise ownership over its digital infrastructure [16]. In the case of AI systems, this control extends to all stages of the data lifecycle: from the data used to train algorithms, to the data explored during operation, and the data generated as output, spanning layers such as Computing, Device, Massive-Data Management, Machine Learning, Modeling, Decision Support, Planning & Acting, and Autonomy/Human-AI Interaction, with ethics cutting across each layer [17].

The concept of digital sovereignty has acquired a large variety of connotations, variants and changing qualities, depending in part, on the self-determination of who is claiming it - state, companies or individuals. In the most prominent category of digital sovereignty claims, the emphasis is on the idea that a nation or region should be able to take autonomous actions and decisions regarding its digital infrastructures and technology deployment [18].

It refers to the need for control over the physical layer (infrastructure, technology), the code layer (standards, rules and design) and the data layer (ownership, flows and use) [19]. Digital sovereignty in this context is both a legal and infrastructural claim: a call not just for jurisdiction, but for the ability to securely store, process, and govern data and digital products in ways that serve national development goals. At the continental level, the Digital Transformation Strategy explores digital sovereignty, while the African Union (AU)'s Data Policy Framework begins to provide a more comprehensive vision on data governance that supports innovation and the better provision of public and private services [20].

For Africans, the concept of digital sovereignty must recognise the economic, logistical, and sustainability realities faced by many countries on the continent: the cost of building and maintaining digital infrastructure, most notably national data centres, is high; resources are often scarce; and the technical burden of large-scale storage can be overwhelming. A single African country cannot reasonably be expected to develop, finance and operate multiple data facilities on its own [21]. This mismatch between ambition and capacity signals the need for a more collaborative vision, one that does not dilute sovereignty but reframes it through solidarity.

Despite a willingness to develop their own approach to digital sovereignty based on their development needs, geopolitical competition and related tensions are reducing the policy space for countries to do this [22]. Indeed, the aspiration to retain control over national data often collides with significant practical limitations and challenges, which undermine the transformative potential of the 4IR, notably a fragmented legal landscape for data protection and severe infrastructural deficits [23].

IV. The Fragmented Landscape of Data Sovereignty in Africa

There are two recognised approaches when discussing data sovereignty in Africa: weak data sovereignty, which relies on minimal state intervention and more open data flows, and strong data sovereignty, a state-led approach with a focus on safeguarding national security [24].

Data sovereignty is a key element of data governance that has a number of critical interlinking pillars, including the differentiation between personal and non-personal data, data localisation, data processing, data protection, cross-border data flows, and data security [25].

In practice, most African states find themselves navigating between these two models without fully embodying either. For example, when global technology companies like Google collect geolocation or behavioural data in countries such as Rwanda or Kenya, this data is rarely stored locally. Instead, it is typically transmitted to and processed within global cloud infrastructures outside the continent, often in jurisdictions where the originating country has no legal or enforcement reach [26].

While Google launched its first African cloud region in Johannesburg, South Africa (SA), in early 2024, providing faster and more secure services for parts of the continent, this infrastructure primarily serves southern Africa [27]. Countries without local hyperscale data centers, such as Rwanda and Kenya, still depend on routing their data to South Africa or to globally distributed data centers in regions like Europe or the U.S [28]. As a result, even with some progress toward regional infrastructure illustrated by Google in SA, data collected in many African countries continues to be governed by foreign jurisdictions, reinforcing the mismatch between the legal ownership of data and the technical infrastructure that stores and processes it. This dynamic further complicates the exercise of data sovereignty and illustrates how infrastructural dependency interacts with fragmented legal regimes to limit Africa's digital autonomy. In other words, while countries like Kenya, Nigeria, and Rwanda have legal provisions that reference safeguards for cross-border data transfers, such as adequacy standards or model contractual clauses, enforcement remains inconsistent, and the uptake of regulatory tools is still limited.

States often exercise data sovereignty to protect the rights of their citizens, most notably through data protection that regulates the use, storage, and cross-border flow of data. Many African countries have enacted national data protection laws; not less than 42 African countries have data protection laws [29].

While instruments such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) signal important steps forward, their ratification and implementation remain inconsistent among member states [29]. The convention does not explicitly mandate data localisation, but its strong emphasis on state sovereignty over personal data has led some countries to adopt national rules that effectively localise data. Similarly, while regional organisations like the Economic Community of West African States (ECOWAS) [30], the East African Community (EAC) [31], and the Southern African Development Community (SADC) have developed national and regional digital policies, these frameworks often lack alignment and technical coherence with one another or are not adequately integrated with continental-level instruments [32].

Many African countries have enacted laws that require data to be stored locally and forbid cross-border transfers of personal data unless authorised by the data protection authorities. For example, in 2017, the Rwandan regulator (Rwanda Utilities Regulatory Authority) fined the MTN Group for failing to move its data center from Uganda in breach of the Regulations Governing Telecom Network Security in Rwanda (2016) that required subscribers' information such as voice, SMS, data including call data records and billing information to be stored and processed in Rwanda [33]. However, not all African countries have the technological capacity or infrastructure, such as data centres, to meet the localisation demands mandated by their laws [34]. An example of this is the Republic of Congo, where the regulatory ambition for localisation was introduced in a context where data infrastructure was still embryonic [35].

Africa's ambition to build an inclusive and serious digital economy is often at odds with a fragmented and uneven legal and infrastructural landscape [36]. This internal disaggregation across jurisdictions, regulatory approaches, technical capabilities, and international alignments directly impedes the continent's collective ability to assert meaningful data sovereignty [37]. At the core of this premise is a fundamental question: how can African states ensure national control over how data is governed, stored and secured, especially when domestic capacity is limited?

Sierzputowski's conception of the Estonian model as sovereign digital extensions housed in foreign jurisdictions through treaty-based extraterritorial arrangements gains particular significance when understood through the lens of trust-based data governance [38]. In Estonia's case, the success of its data embassy with Luxembourg was not merely legalistic but rooted in the existence of a trusted corridor: a convergence of shared legal frameworks, mutual political confidence, and aligned digital infrastructure standards. This corridor enabled the practical enforcement of extraterritorial data sovereignty in a context of regulatory coherence and geopolitical stability [39]. The Estonian model has run without incident since 2017, prompting other countries to explore the data embassy option with Luxembourg [40].

However, such enabling conditions are not easily replicable elsewhere.

India, for example, has assessed the prospect of establishing data embassies to facilitate nationwide technological development and allow data centers to take advantage of global infrastructure that provides maximum reliability and resiliency through a distributed data storage architecture. As part of its Draft National Data Governance Framework Policy (May 2022), India's Ministry of Electronics and Information Technology (MeitY) proposed developing centralised data repositories for secure sharing between government entities within the country, to be managed by the India Data Management Office (IDMO) [41]. In exploring these arrangements, however, the country faces considerable uncertainty regarding diplomatic protections for state data, the legal treatment of extraterritorial digital assets, and the reliability of cross-border hosting partners [42]. These concerns are compounded by the lack of a formalised corridor of trust. India has yet to establish the kind of bilateral digital and legal alignment that underpinned Estonia's partnership with Luxembourg.

If the Estonian model is to be replicated on the continent, it would require the development of interoperable legal instruments, binding interstate agreements, and reliable regulatory institutions that engender corridors of trust.

V. Critical Digital Infrastructure and the Existing Limitations

The African Union has recommended the need to cooperate on regional and continental data infrastructure to host advanced data-driven technologies (such as Big Data, Machine learning and AI) [43]. Furthermore, heads of state committed to "establish regional data centers with high-performance computing connected through a continental high-speed network and build robust cybersecurity measures to safeguard data integrity and resilience, optimising compute resources with a minimal carbon footprint [44]." The region is witnessing rapid growth, driven by increased investments and expanding digital infrastructure, which is notable given the projected 25 to 30 percent annual growth in data demand over the next five years [45]. According to the Africa Data Centres Association, meeting this demand would require the continent to add at least 700 new data centre facilities and develop an additional 1,000 megawatts (MW) of capacity, targets that, in the absence of coordinated regional strategies, are unlikely to be met by fragmented national initiatives [46]. To illustrate the scale of this energy need, 1,000 MW could potentially power between 650,000 and 1 million African households, depending on average home consumption levels, an especially significant figure in a region where over 600 million people currently lack access to reliable electricity [47].

The continent's ambitions in AI infrastructure are further illustrated by plans for Africa's first AI factory, a joint initiative that may involve investments of up to USD 720 million, developed by Cassava Technologies in partnership with Nvidia Corporation [48]. The facility aims to deploy AI-powered data centres in South Africa, Egypt, Nigeria, Kenya, and Morocco, with the pilot project commencing in South Africa, where 3,000 Nvidia Graphics Processing Units are expected to be installed by June 2025 [49].

Despite the continent's growing digital ambitions and expanding internet penetration, however, Africa's data infrastructure remains critically underdeveloped relative to global benchmarks. As of mid-2025, the African continent is home to approximately 208 data centers across 37 countries, representing less than 1% of global data center capacity [50].

Despite an emergence of local cloud providers like Nebula [51], which are better positioned to understand and comply with national data protection laws and can offer more cost-efficient solutions [52], as well as global players looking to adapt to local requirements [53], the majority of African countries still depend on hyper-scale cloud providers, with data ultimately physically stored on servers located in data centers around the world, which contradicts the very concept of data sovereignty [54]. While one might suggest that these global providers could adopt data embassy-like principles, such arrangements would lack the enforceability and jurisdictional guarantees provided by formal state-to-state agreements. Data embassies, by design, derive their legal inviolability from bilateral treaties anchored in international law, particularly the VCDR, which private companies cannot replicate.

Even when a cloud provider claims to uphold data sovereignty, those commitments remain contractual, not diplomatic, and are vulnerable to override by the provider's domestic legislation, such as the U.S. CLOUD Act [55]. As a result, without intergovernmental agreements, the risk of foreign interference or loss of jurisdictional control persists, reinforcing the need for African states to explore more sovereign, treaty-based approaches to cross-border data hosting. The absence of data centres and control over their construction hampers a nation's ability to maintain digital sovereignty and the right to self-determination [56].

Data centres, while strategically vital for data sovereignty and the development of critical digital infrastructure, are prohibitively expensive to build and operate in many African countries. The average cost of developing a 1 MW data centre hovers around USD 10 million, and in higher-cost environments such as Nigeria, this figure can reach USD 15 million per MW due to infrastructure gaps, higher operational risks, and dependency on expensive imported hardware. These figures become even more daunting when viewed against the backdrop of foreign exchange (FX) volatility [57]. FX crises, common across many African economies, compound the cost of importing key components such as servers, cooling systems, and networking equipment, while also disrupting project timelines and increasing long-term maintenance burdens [56].

As a result, domestically hosted data services in Africa are often significantly more expensive than their global counterparts [57]. Data hosting costs in many African countries are two to three times higher than in Europe or North America, primarily due to energy supply inconsistencies, connectivity limitations, and reliance on foreign-manufactured hardware [58].

This cost asymmetry undermines the case for localisation, as storing data abroad becomes not only cheaper, but also more technically viable. It creates a profound regulatory paradox with states demanding local data storage as a matter of sovereignty and national security, yet simultaneously fostering conditions that incentivise external storage due to infrastructural underdevelopment and market pricing inefficiencies. Insufficient capital for infrastructure development poses complex challenges for most African nations, thus leading to unequal economic, political, and cultural power, threatening the sovereignty and national security of many countries and regions [59].

Even in countries viewed as digitally progressive, the burden of building and maintaining large-scale infrastructure often requires heavy reliance on foreign capital and partnerships, which can dilute the intended goals of sovereignty. A case in point is Kenya, where Microsoft and the UAE-based AI technology firm G42 announced a $1 billion investment package that includes a "green" data centre to support the Microsoft Azure East Africa Cloud Region and leverage Kenya's renewable energy achievements [60]. This development represents one of the largest single investments in digital infrastructure in the region's history. Yet, some analysts have noted, Kenya, the largest economy in East Africa, currently lacks the domestic data volume necessary to fully utilise this facility, at least in the near to medium term [61].

The economic logic of such projects, while potentially transformative in the long run, does not necessarily align with immediate local data needs [62]. Rather, these large-scale investments often serve broader geostrategic interests, such as establishing regional dominance in AI, capturing cloud markets, or securing training grounds for large language models.

At the same time, the host country remains structurally dependent on foreign technology, expertise, and jurisdictional uncertainty and there is a fear that more dominant nations can take advantage of Africa's weak political institutions and limited digital-savvy population to pursue their geopolitical objectives on the continent [63].

Beyond the cost implications, political instability and conflict render some countries unsuitable for significant data center investments due to the inherent risks to infrastructure and operations [64]. For example, Sudan's ongoing conflict has severely damaged its digital infrastructure, highlighting the fragility of digital systems in unstable environments [65]. One could wonder what happens if data is compromised due to circumstances beyond the host country's control, such as war, terrorism, or natural disasters? While traditional data centers are vulnerable to these risks, data embassies offer a potential safeguard by legally situating critical data in politically stable jurisdictions under the diplomatic protection of the sending state, thereby mitigating exposure to such local disruptions. This approach requires carefully negotiated bilateral agreements and serious contingency planning to address unforeseen compromises. Landlocked countries must rely on coastal neighbours for core internet infrastructure, sometimes in politically volatile regions [66], leading to localisation attempts to bridge latency speeds, often without the necessary domestic capacity. Digital continuity is critical and the ability to secure the operation of government electronic services covered exterritorially by the sovereignty of a native state according to international laws should be an option considered in the event of conflict [67].

Critically, modern data centres must be state-of-the-art, high-capacity, power-efficient and climate-resilient [68]. Building for sustainability, given that the critical part of data centre operations requires significant energy consumption and cooling, aligns with environmental, social, and governance (ESG) best practices, and the UN's Global Digital Compact Objective 1 that calls for promoting sustainability across the entire life cycle of digital technologies [69].

Building for sustainability also recognises the current climate-related challenges faced by many African nations that affect natural resources, such as water bodies. As AI systems and services increase their size and scale, demanding increasing amounts of computational power, there is a growing call from human rights and environmental rights advocates to mandate tech companies to report on the energy and water consumption for their data centres, given the risk of causing irreparable damage to the environment, displacing individuals, and affecting land rights [70]. With jurisdictions such as the EU and the US introducing legislation requiring mandatory disclosure of environmental impacts tied to data center operations, these demands highlight the need for Africa, where digital infrastructure is still emerging, to proactively embed environmental transparency and sustainability safeguards within its data governance strategies, including future adoption or adaptation of the data embassy model [71].

Lastly, many countries suffer from unreliable and insufficient power supplies, which pose a significant challenge to operating modern data centres and with continuity. The Republic of Congo, for example, had no nationally recognised tiered data centre capable of securely storing and managing personal data at scale until 2022 [72]. The launch of the national data centre in Brazzaville, constructed with Chinese technical assistance, was a major milestone [73]. However, the centre's operational capacity remains limited both in volume and sophistication. According to the BTI Transformation Index, a program by Bertelsmann Stiftung, much of the country's data infrastructure relies on unstable energy sources, intermittent connectivity, and inconsistent maintenance protocols that significantly hinder the secure storage and continuous processing of data [74]. In Nigeria, data center power needs often exceed the country's total national grid generation capacity, driving up the cost of energy [75]. Experts warn that these broadband and data centre gaps threaten Nigeria's goal of achieving a $1 trillion economy [76]. There is a push to design data centers with in-built power sources, such as natural gas, renewable energy sources, or diesel generators, to ensure uptime, which further increases operational costs that are then passed on to consumers [77].

Rack Centre, for example, powers its new data hub with natural gas to ensure reliability [78]. Similarly, Africa Data Centers (ADC) in South Africa employs a hybrid energy model combining solar, generators, and grid power, while Onix Data Centre in Ghana is exploring greener backup systems to address electricity shortfalls [79].

The above exemplifies a broader dilemma: sovereignty concerns oftentimes outpaces infrastructural and regulatory capacity, rendering them symbolic rather than operational. These systemic constraints highlight the need for alternative governance and infrastructure-sharing models that can reconcile national sovereignty with economic realities in the medium term, thereby meeting the rapid adoption of data-intensive technologies in the 4IR.

This infrastructural lag reveals the strategic disconnect between the Estonian model of data embassies, as defined by Sierzputowski, and the material capabilities required to enforce them. In much of the continent, national policies are increasingly promoting sovereign data control and in-country storage mandates; however, the technical capacity to support such objectives remains elusive [80]. The Estonian approach presumes the existence of strong domestic infrastructure and comprehensive digital continuity [81]. This means that Estonia mirrors critical state data in a foreign facility, specifically in Luxembourg, which is granted sovereign status through a form of bilateral treaty [82]. What enables this model to function effectively is that both Estonia and Luxembourg operate under shared legal frameworks, including adherence to the GDPR and other digital laws, ensuring that data stored abroad receives the same level of protection and recognition as if it were on Estonian soil [83]. Again, the mutual political confidence, with both governments demonstrating strong diplomatic trust and a shared commitment to cybersecurity, digital innovation, and the protection of critical assets, facilitates the operationalisation of these agreements [84]. Moreover, the success of this initiative is made possible by the aligned digital infrastructure standards both nations share. Luxembourg's highly secure, state-of-the-art data centers meet Estonia's strong operational and cybersecurity requirements, allowing for a smooth technical integration and the practical enforcement of extraterritorial data sovereignty [85]. These conditions: legal harmony, political trust, and advanced infrastructure, were essential for the Estonian data embassy model to be viable and secure.

VI. Challenges of Implementing the Data Embassy Concept in Africa

The proposed implementation of data embassies in Africa rests on a nuanced interpretation and extension of established international legal principles, particularly those enshrined in the VCDR of 1961 [86]. Despite the conceptual appeal, significant legal, technical and operational challenges exist in establishing data embassies in the African context.

- **Legal Capacity:** Establishing a data embassy involves a complex and diplomatically intensive legal foundation, primarily relying on formal intergovernmental treaties that confer extraterritorial legal status to digital infrastructure. While based in the spirit of the VCDR, the Estonia–Luxembourg model demonstrates that such frameworks must be augmented by specific bilateral agreements to ensure legal clarity and enforceability. Unlike Estonia, a (small) digitally mature, highly integrated, and politically stable state, many African states currently lack the legal capacity, negotiating leverage, or diplomatic infrastructure to negotiate and enforce such high-level agreements, particularly with technologically advanced host nations.

- **Interpretive Challenges of VCDR:** The VCDR was drafted in a pre-digital era, with "premises," "archives," and "documents" understood primarily in a physical sense, and whether these terms automatically extend to cloud servers, encrypted databases, or third-party-operated data centers without explicit agreement remains legally untested [87]. As such, inviolability and legal immunity of digital assets would almost certainly require supplementary legal instruments, such as dedicated bilateral treaties, rather than an automatic extension of VCDR protections [88].

- **Expropriation:** Another challenge in implementing the data embassy concept in Africa lies in the potential risk of expropriation or unilateral interference by host states. In politically unstable or weakly institutionalised environments, the legal guarantees of extraterritoriality may be difficult to enforce, particularly in the absence of effective rule of law and judicial independence. Without strong dispute resolution mechanisms and binding international agreements, there remains a risk that a host country could, in times of crisis or shifting political interests, seize, access, or suspend the operation of foreign-owned digital infrastructure amounting to a form of digital expropriation. This risk undermines the core purpose of data embassies: to ensure the sovereign control, integrity, and continuity of state data, even beyond national borders.

- **Legal Fragmentation:** The effective implementation of data embassies in Africa hinges on the existence of robust legal infrastructure both in terms of harmonised regulatory environments and binding mechanisms for resolving disputes. However, fragmentation across national legal systems significantly complicates the operationalisation of any unified data embassy framework. While regional instruments such as the Malabo Convention provide a foundational legal blueprint, their limited ratification and uneven implementation have left African states with a patchwork of divergent data governance laws, undermining trust, interoperability, and mutual legal recognition.

- **Inadequate Dispute Resolution Mechanisms:** Compounding the challenge of legal fragmentation is the absence of clear, legally binding, and procedurally sound dispute resolution mechanisms within most national or regional systems. Such mechanisms are critical to address breaches of inviolability, jurisdictional conflicts, or interpretive disagreements between sending and host states, especially during geopolitical tensions or emergency access scenarios. Yet key legal questions remain unresolved: Which courts or tribunals will have jurisdiction in the event of a dispute?

Do domestic or regional judicial systems possess the necessary technical expertise to adjudicate data-centric conflicts involving access, cybersecurity, or extraterritorial claims? And more fundamentally, how can violations such as unauthorised access or delayed data restoration be objectively quantified and proven in legal terms?

These gaps highlight the urgent need for capacity-building within African judicial systems, the development of model arbitration clauses, and the creation of specialised regional dispute resolution protocols or tribunals capable of providing impartial and predictable legal recourse. Without such instruments, the credibility, enforceability, and strategic value of data embassies as sovereignty-preserving mechanisms may be significantly diminished. Equally important is the need for African legal systems to embrace innovation in order to respond to the novel challenges presented by digital sovereignty. This includes cultivating jurisprudence through the development of case law, as well as encouraging courts to engage proactively with emerging technologies and treaty-based instruments like data embassies. Legal infrastructure is not merely about codified rules; it also depends on political and institutional will. Strengthening the capacity of courts to set precedent and adapt legal reasoning to digital-era sovereignty claims will be essential for legitimising and enforcing such models within Africa's complex governance landscape.

- **Establishing Corridors of Trust:** The successful implementation of data embassies hinges not merely on legal doctrine but on the construction of robust corridors of trust between states. While the VCDR offers foundational principles such as inviolability of premises and archives, it is not, on its own, sufficient to govern the complexities of sovereign digital infrastructure hosted abroad. As demonstrated in the Estonia–Luxembourg case, a dedicated bilateral agreement was essential to clarify obligations, dispute mechanisms, and operational safeguards. Beyond legal architecture, mutual trust is indispensable. The sensitive nature of state data demands strong cybersecurity frameworks, legal certainty, and credible privacy assurances from the host state.

As noted in India's exploration of the concept, establishing a data embassy requires building an environment of trust, reinforced by transparent governance and verifiable protection standards. In the African context, where digital cooperation often occurs in the shadow of political volatility, institutional fragmentation, and uneven enforcement capacity, establishing corridors of trust would require more than bilateral treaties. It would necessitate the development of regionally anchored norms and safeguards, possibly under the umbrella of the African Union or regional economic communities that can endure leadership transitions, security crises, and shifting geopolitical alliances. Here, corridors of trust become both a legal and political infrastructure, one that reinforces shared accountability, builds technical confidence, and ensures that no single state bears the burden of trust alone.

- **The Fragility of Political Will and the Risks of Host-State Dependence:** While legal frameworks are essential to the operation of data embassies, their efficacy ultimately depends on the political restraint and good-faith cooperation of the host state [98]. The principle of diplomatic inviolability, foundational to the concept of data embassies, hinges not only on legal recognition but also on a shared political commitment to uphold treaty obligations. However, history shows that political will can override legal protections, particularly when host states perceive grave national interests or security threats. The 1979 Tehran Hostage Crisis [89] and the 2024 Ecuadorian Embassy Raid, in which Ecuadorian authorities forcibly entered the Mexican embassy in Quito, serve as stark reminders that even long-established diplomatic norms under the VCDR can be violated when political motives prevail [90]. In the African context, this risk is amplified by political instability and uneven institutional governance in some regions. The long-term commitment required to uphold sovereign digital infrastructure, especially infrastructure embedded in cross-border or treaty-based mechanisms, may be undermined by leadership transitions, shifting national interests, or regional realignments.

In such scenarios, the inviolability of a data embassy could be unilaterally revoked, challenged, or ignored, especially during domestic crises or geopolitical tensions [91]. Ironically, while data embassies are designed to enhance data sovereignty, they may introduce a new layer of dependency on the political posture of the host country, potentially exposing critical national data assets to foreign control or intervention during moments of instability.

- **Enabling Requirements for Host States:** Establishing a data embassy demands a host country with highly resilient and secure data center infrastructure, typically meeting Tier IV standards for uptime and redundancy [92], consistent power, in addition to the increasing need to build for sustainability. While some African countries are emerging as data centre hubs (for example, South Africa, Kenya, Nigeria), consistent, high-quality grid power, robust connectivity, and strong cybersecurity ecosystems are not uniformly available across the continent [93]. This limits the pool of potential host states within Africa and supports the case for considering trusted external partners as well, at least in the short to medium term.

- **Replication:** Best practices in data storage require data to be replicated in multiple geographical locations to avoid data loss due to catastrophic failures. There is a risk that if data is stored in one data center located in the host country, personal data from all vendors of the home state could be lost. There are two potential solutions that may mitigate this risk. The first is to establish multiple data repositories. In essence, these third countries serve as a back-up. The advantage of having a back-up in another country is that the host country can then not hold the data of the home state "hostage; the data owner can back-up in the third country. This solution has a number of challenges: (a) different geographical areas that mirror the data could further increase the cost of data sovereignty and would be prohibitive for small or poorer countries; (b) the two countries (host country and third party country) may collude against the home state; and (c) this arrangement requires treaties among multiple countries, increasing the complexity and cost.

It also requires both data centres to be secure thereby increasing the vulnerability of the data being hacked into or leaked.

A second potential solution is to create data centers in a small number of countries with the data from each country being shared across these data centers. Such a 'round robin'-type of arrangement would result in sufficient deterrents by a country from unilaterally strong-arming another. It has the advantage of spreading the risk and minimizing the potential for data "hostage-taking" and/or collusion. The advantage of this setup is that (a) all countries participating in such a consortium gain from economies of scale; (b) countries having specialist skills can supply their skills while enjoying the complementary skills from specialists in other countries with respect to constructing and maintaining the data center; and (c) smaller countries can participate in the consortium while not hosting any data but gaining protection from one country due to the consortium's embassy rules. However, this solution is not immune from challenges; it is still conceivable that the set of countries could collude against a "victim" country as a result of geopolitics or other incentives. There is also the issue of increased cost if each country sets up a data center in order to be part of this round robin, which goes against the premise of the data embassies concept and its promise to minimize infrastructural costs.

- **Cybersecurity:** Embassies are secured using multi-layered physical, human, and technological defenses because they are high-value targets for espionage, protests, and terrorism. Typically, the host country, in collaboration with the foreign country, whose embassy secures embassies. Digital embassies similarly need to be secured. With respect to securing the information, the country employing the data embassy can install its own software and encrypt the data such that it will be near impossible for the host country or hackers from a third country to decode the data. However, the second and third parties can engage in denial of service attacks and prevent access to the data or even be able to destroy the data from remote third-party countries. The ability to set up, maintain, and run these data centers securely requires an efficient, experienced, well-educated, and well-trained work force some of whom must be on-site in the hosting country because bugs and vulnerabilities may be discovered overnight and only prompt responses can thwart attacks by third parties that seek to destroy or damage the data resulting in several hours of downtime, lost data, and huge losses to the country whose data it is. How many African countries have and can employ such a skilled workforce and have the means to enable international-level cybersecurity on a large-scale at cost that are viable commercially potentially on data related to everyday commerce for a whole country is a question we have to answer before we can deploy such solutions broadly.

- **Foreign Dominance:** Pursuing digital sovereignty in a world dominated by technological giants presents formidable challenges for African states. The digital ecosystem cloud services, data centers, cybersecurity tools, and AI infrastructure is largely controlled by a handful of powerful multinational corporations and states, many of which operate beyond the regulatory reach of African jurisdictions. While donor-funded or externally driven digital projects may offer short-term infrastructure gains, they are often double-edged swords: accompanied by opaque contracts, embedded foreign standards, and long-term dependencies that undermine national control over data flows, security policies, and strategic autonomy. This asymmetry weakens the capacity of African states to protect their digital sovereignty and, by extension, their territorial integrity in the digital domain. Without a shift toward regionally owned infrastructure, legal harmonisation, and indigenous innovation, Africa risks becoming a passive consumer of foreign technologies, rather than an active shaper of its own digital destiny [94].

- **Limited Technical Expertise:** Operating and maintaining a data embassy requires significant technical expertise in cybersecurity, data management, and network security from both the sending and receiving states. Developing and retaining such highly skilled personnel remains a challenge in many African countries [95]. Moreover, attracting this level of talent may be more feasible and even more cost-effective through regional or international cooperation, where the necessary expertise may be more readily available.

In some cases, it may be more difficult to build this capacity domestically than to access it through trusted partnerships. Ensuring advanced cybersecurity measures, including protection against sophisticated cyberattacks and insider threats at the host location, is paramount to prevent data breaches or unauthorised access.

The key technical challenges that need to be resolved and for which technical expertise is needed are as follows:

1. Cross-Jurisdictional Encryption and Key Management: Host-country laws or surveillance regimes may demand access or limit cryptographic autonomy.
2. Physical Security Integration with Digital Controls: Maintaining embassy-level physical security (air gaps, EM shielding, controlled access) in a foreign data center is complex.
3. Sovereign Control Over Infrastructure: Using third-party cloud or colocation providers creates a dependency on foreign software, firmware, or network layers.
4. Secure Remote Operations: Remote administration must be resilient to man-in-the-middle attacks and insider threats.
5. Zero Trust and Network Isolation: Enforcing strict network segmentation and least-privilege access while allowing functional interoperability.
6. Data Sovereignty and Backup: Secure data replication and backup across borders must ensure immutability and legal compliance.
7. Supply Chain Security: Attacks at the firmware or microcode level are difficult to detect and mitigate post-deployment.

Funding limitations: While the Africa Declaration on Artificial Intelligence rightly commits to strengthening sovereign compute infrastructure, regional data centers, and a $60 billion Africa AI Fund [96], there remains significant uncertainty around how such ambitious infrastructure, including emerging concepts like data embassies, will be financed and sustained in practice. Practical mechanisms for pooling funds regionally, especially for politically sensitive, sovereignty-linked infrastructure are still lacking. Although the Declaration calls for regional collaboration and investment in shared infrastructure, it does not spell out how the Africa AI Fund or other instruments will specifically address cross-border arrangements, protect equitable cost-sharing, or prevent imbalances where only a few countries bear the operational and maintenance burden.

Despite these challenges, the very novelty of data embassies in Africa presents a strategic opportunity for African states to co-design bespoke legal and operational frameworks suited to their own developmental trajectories and governance needs. However, existing definitions of data embassies, largely shaped by the Estonian model and grounded in diplomatic extraterritoriality, are not fully adequate for the African context. They presuppose a level of legal uniformity, infrastructure maturity, and political stability that many states on the continent are still in the process of building. As such, the concept must be reframed: not as a direct replication of European models, but as a flexible, regionally anchored mechanism that prioritises shared sovereignty, legal interoperability, and infrastructural co-investment. Reframing the definition in this way opens the door to more inclusive, resilient, and trust-based approaches to digital sovereignty across Africa.

VII. Recommendations

While data embassies are not a silver bullet for Africa's digital sovereignty challenges, they present a promising, controllable, and geopolitically resilient model, if pursued with rigor, caution, and a long-term strategic lens. A successful implementation requires alignment between law, technology, diplomacy, and public trust. African nations have a unique opportunity to lead in defining the global norms for sovereign digital infrastructure that transcends borders.

We propose the following comprehensive recommendations:

1. Enforcing Regional and Continental Legal Frameworks through Political Will and Mutual Trust

- Harmonise digital sovereignty principles across the African Union (AU) and regional economic communities (RECs), incorporating data embassies into future revisions of the *Malabo Convention (2014)* and related treaties.

- Develop intergovernmental protocols for cross-border data storage, clearly defining jurisdiction, access rights, and accountability.
- Standardise definitions for "sovereign data," "critical infrastructure," and "cyber hostilities" to reduce ambiguity in enforcement.

2. Invest in Cryptographic and Zero-Trust Architectures

- Deploy sovereign key management systems with remote attestation and geo-fencing to ensure that control of encryption keys always remains with the data-owning nation.
- Use confidential computing, homomorphic encryption, and zero-knowledge proofs to ensure data remains verifiable but inaccessible to foreign hosts.
- Implement zero-trust security models within embassy environments, including fine-grained access controls, continuous authentication, and east-west traffic segmentation.

3. Build African-Owned Data Centers and Hybrid Models

- Prioritise intra-African data embassies hosted in trusted partner states, leveraging existing political and cultural alliances while attempting aggressively to enable agreements among countries across the continent.
- Encourage public-private partnerships to fund Tier III+ data centers in strategic African locations under sovereign ownership, but with optional offshore replication.
- Create multi-location hybrid architectures, where sensitive services may remain onshore when possible while other data and mirrored backups are hosted in data embassies.

4. Ensure Host-State Agreement Transparency and Resilience

- Negotiate diplomatic-grade hosting agreements that embed Vienna Convention-like protections for data infrastructure and operations seeking explicit legal agreements between countries accepting that such protections extend to data-related infrastructure and the data.
- Include termination clauses, backup contingencies, and incident response protocols for scenarios such as regime change, war, or legal conflict in the host country.

5. Enhance Cybersecurity Readiness and National Capacity

- Build national cybersecurity operations centers (CSOCs) with continuous visibility into data embassy infrastructure.
- Train and retain elite teams in cyber forensics, secure software engineering, and defensive operations to manage remote and sovereign-hosted assets.
- Adopt supply chain verification tools and hardware root-of-trust mechanisms for embassy infrastructure.

6. Foster International Norms and Strategic Diplomacy

- Work with the UN, ITU, and World Bank to promote data embassy recognition as a sovereign extension of state infrastructure in the digital realm.
- Advocate for African interests in global data governance negotiations, emphasising equitable access, non-interference, and digital non-alignment.
- Develop pan-African diplomatic cyber doctrines to navigate conflicts involving data embassies, espionage, or extraterritorial subpoenas.

7. Establish Mirror Legal Oversight Bodies in Both Home and Host Countries to Resolve Disputes and ensure transparent audit trails.

- Work with the UN, ITU, and World Bank to promote data embassy recognition as a sovereign extension of state infrastructure in the digital realm.
- Create parallel oversight institutions in both the data-hosting and data-owning states to manage legal compliance, resolve disputes, and preserve sovereignty.
- Ensure mechanisms for joint accountability and transparent audit trails, reinforcing trust and operational integrity in bilateral or regional data embassy arrangements.

8. Develop and Test Disaster Recovery and Continuity Plans

- Integrate data embassies into national continuity of government (COG) plans, simulating scenarios like internal network collapse, election crises, or infrastructure sabotage.

- Design automated failover systems that can re-route critical services to embassies within minutes without compromising data integrity or public access.
- Ensure secure, redundant backups are maintained both in-country and offshore to survive catastrophic data loss.

9. Engage Citizens and Civil Society
- Launch public communication campaigns to clarify how data embassies protect privacy, prevent foreign surveillance, and support national resilience.
- Involve civil society and academia in auditing the data embassy model for ethics, accountability, and inclusivity.
- Guarantee that citizen rights to data protection and redress are not weakened by offshore storage, especially for marginalised populations.

10. Measure and Monitor Impact
- Establish performance metrics for data embassies, including availability, incident response time, latency, auditability, and cost-efficiency.
- Conduct independent security audits and technical peer reviews at regular intervals.
- Compare the effectiveness of data embassies with alternative sovereignty-preserving models (e.g., cloud neutrality zones, data trusts, edge computing).

VIII. Conclusion

Africa stands at a pivotal juncture in its digital transformation. While emerging technologies such as AI promise to accelerate development, the continent continues to grapple with deeply entrenched challenges, notably: fragmented data governance regimes and critical infrastructural deficits. These challenges risk undermining Africa's efforts to assert digital sovereignty and fully harness the potential of the Fourth Industrial Revolution.

The data embassy model, as pioneered by Estonia, offers a compelling framework for safeguarding critical state data through diplomatically protected extraterritorial hosting arrangements. It provides resilience in times of crisis and ensures continuity of digital government functions.

However, transposing this model directly onto the African context without adaptation risks obscuring the continent's unique legal pluralism, infrastructural limitations, and political volatility. Estonia's success was not solely grounded in legal doctrine but in sturdy institutions, technical maturity, and a carefully negotiated bilateral agreement with Luxembourg conditions that captured the spirit of the VCDR.

In Africa, where data protection laws remain fragmented, digital infrastructure is unevenly distributed, and regional trust frameworks are still emerging, the definition of data embassies must be reframed. Instead of viewing them as fixed extensions of national sovereignty abroad, they must be conceptualised as regional sovereignty-sharing mechanisms, flexible arrangements grounded in trust, co-investment, and harmonised legal frameworks. This shift would require embedding such initiatives within continental instruments like the Malabo Convention, supported by regional institutions such as the African Union. Only then can Africa move from being a passive consumer of external digital governance models to becoming an active architect of its own digital future.

Currently, the data embassy concept remains underdeveloped for Africa's specific needs. Its normative potential is clear, but its practical, legal, and infrastructural feasibility across the continent remains insufficiently explored. As this paper has shown, the model must evolve if it is to align with the realities and aspirations of African states.

This reflection gives rise to a broader empirical research agenda that cuts across legal, technical, and policy domains. Several key questions emerge, most notably:

- Drawing from international experiences, particularly Estonia's, what elements of the model are transferable, and which require redesign?
- How can the principles of the VCDR be reinterpreted or adapted to support regional data sovereignty initiatives in Africa, particularly in light of the continent's infrastructural and legal challenges?
- What practical legal, institutional, technical, cybersecurity, infrastructural, risk management, and liability frameworks are necessary to design and implement secure, sovereign, and sustainable data embassy arrangements or their functional alternatives within the African context?

These are not merely academic inquiries; they go to the heart of how Africa envisions and exercises digital sovereignty. Whether through reframed data embassies or entirely new regional mechanisms, the continent must chart a path that reflects its institutional capacities, developmental goals, and collective interests. This calls for sustained engagement from researchers, legal experts, technologists, and policymakers, and a commitment to developing African-led solutions for a digital future that is secure, sovereign, and inclusive.

Acknowledgments

The authors would like to acknowledge the contributions of Fabro Steibel, Kenneth Muhangi, and Raymond Ononiwu, who provided technical and policy feedback. The views expressed in this article are those of the authors and do not necessarily reflect the views of their respective institutions or their affiliates.

References

[1] Sierzputowski, B. (2019), The data embassy under public international law—Erratum. International and Comparative Law Quarterly, 68(04), 777. https://doi.org/10.1017/s0020589319000137

[2] Sierzputowski, 2019 n 1).

[3] Sierzputowski, 2019.

[4] Sierzputowski, 2019.

[5] See, for example, Article 1(b) and Article 2(2) of the Agreement dated June 20, 2017, between the Republic of Estonia and the Grand Duchy of Luxembourg on hosting Estonian data and information systems, which states that Luxembourg shall make available to Estonia a dedicated data centre space for the lease cost agreed upon by the competent authorities. The Agreement defines the "premises" as space intended specifically for hosting Estonian data and systems, thereby creating obligations akin to those associated with diplomatic premises.

[6] Soulé, F. (2024). Digital Sovereignty in Africa: Moving beyond Local Data Ownership. In Policy Brief No. 185 — June 2024. https://www.cigionline.org/static/documents/PB_no.185.pdf

[7] Benamara, A. (2025, February 27). *EXCLUSIVE Q&A: Africa's blueprint for a secure digital future*. TechAfrica News. https://techafricanews.com/2025/02/27/exclusive-qa-africas-blueprint-for-a-secure-digital-future/.

[8] Republic of Estonia & Grand Duchy of Luxembourg. (2016). Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems. https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_ment.pdf

[10] Sierzputowski, 2019.

[11] Republic of Estonia & Grand Duchy of Luxembourg, 2016, Arts. 22, 24.

[12] Bartholomeusz, L. (2009). Eileen Denza. Diplomatic Law, Commentary on the Vienna Convention on Diplomatic Relations. European Journal of International Law, 20(4), 1286–1288. https://doi.org/10.1093/ejil/chp082.

[13] (Bartholomeusz, 2009)

[14] Vienna Convention on Diplomatic Relations. (1964). United Nations Treaty Series, 500, 95. https://treaties.un.org/doc/Publication/UNTS/Volume%20500/v500.pdf
Republic of Estonia & Grand Duchy of Luxembourg. (2018). Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the hosting of data and information systems (Entered into force July 1, 2018). https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf

[15] Republic of Estonia & Grand Duchy of Luxembourg, 2016, Arts. 8.

[16] Continental Artificial Intelligence Strategy. (2024). In United Nations Educational, Scientific and Cultural Organization, Continental Artificial Intelligence Strategy. https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf

[17] Fleming, S. (2025, January 10). *What is digital sovereignty and how are countries approaching it?* World Economic Forum. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

[18] IEEE SA. (2024, August 21). The IEEE Global Initiative 2.0 on Ethics of Autonomous and Intelligent Systems - IEEE Standards Association. IEEE Standards Association. https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/

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

[20] Musoni, M., Karkare, P., Teevan, C., Domingo, E., & The centre for Africa-Europe relations. (2023). Global approaches to digital sovereignty: Competing definitions and contrasting policy (Discussion Paper No. 344).

[21] Musoni et al., Global Approaches to Digital Sovereignty, Discussion Paper No. 344 (2023).

[22] Bryant, J. (2021). Africa in the information age: Challenges, opportunities, and strategies for data protection and digital rights. Stanford Technology Law Review, 24, 389–412. https://law.stanford.edu/wp-content/uploads/2021/05/BryantAfricaInTheInformationAge.pdf

[23] Musoni et al., Global Approaches to Digital Sovereignty, Discussion Paper No. 344 (2023).

[24] Media Defence. (2025, February 23). Data privacy and data protection – Sub-Saharan Africa. https://www.mediadefence.org/resource-hub/data-privacy-protection-sub-saharan-africa/.

[25] African Union. (2022). AU Data Policy Framework. https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf

[26] African Union, 2022.

[27] Kabanda, S. M., Cengiz, N., Rajaratnam, K., Watson, B. W., Brown, Q., Esterhuizen, T. M., & Moodley, K. (2023). Data sharing and data governance in sub-Saharan Africa: Perspectives from researchers and scientists engaged in data-intensive research. South African Journal of Science, 119(5/6). https://doi.org/10.17159/sajs.2023/15129 .

[28] Patel, N. (2024, January 31). New Google Cloud region now open in Johannesburg. Google Cloud Blog. https://cloud.google.com/blog/products/infrastructure/heita-south-africa-new-cloud-region.

[29] Muhammed, J. (2025, May 2). Africa's Digital infrastructure: Why data centres are the new oil. African Leadership Magazine. https://www.africanleadershipmagazine.co.uk/africas-digital-infrastructure-why-data-centres-are-the-new-oil/

[30] Tsebee, D., Oloyede, R., Tech Hive Advisory Limited, & Center for Law & Innovation. (2025). State of AI regulation in Africa: Trends and developments [Report]. Tech Hive Advisory & Center for Law & Innovation.https://cdn.prod.website-files.com/641a2c1dcea0041f8d407596/67ebe308d179638db4072654_State%20of%20AI%20Regulation%20in%20Africa%20Trends%20and%20Developments%20v2_.pdf.

[31] African Union, 2022.

[32] Economic Community of West African States. (2010). Supplementary Act A1SA.1F01F10 on personal data protection within ECOWAS. https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf

[33] East African Community Legal Framework for Cyberlaws

[34] EAC set to advance Data Governance and Protection with development of a regional Policy Framework. (2024, October 25). https://www.eac.int/press-releases/3195-eac-set-to-advance-data-governance-and-protection-with-development-of-a-regional-policy-framework

[35] Uwiringiyimana, C. (2017, May 17). Rwanda regulator fines MTN Rwanda $8.5 mln over external IT hub. Reuters. https://www.reuters.com/article/business/finance/rwanda-regulator-fines-mtn-rwanda-85-mln-over-external-it-hub-idUSL8N1IJ2IJ/.

[36] Svantesson, D., Jerker, D., Svantesson, B., & Kuner, C. (2020). Data localisation trends and challenges. OECD Digital Economy Papers. https://doi.org/10.1787/7fbaed62-en

[37] BTI 2024 Congo, Rep. Country Report. (n.d.). BTI 2024. https://bti-project.org/en/reports/country-report/COG

[38] Edun, S. (2024). Digital economies: Challenges and opportunities in Africa. Africa Data Centres Association. Retrieved July 10, 2025, from https://www.idc-a.org/insights/rYTDOeOgoit4csjfZnuR .

[39] This observation draws on several sources that highlight the disconnect between national and regional data governance efforts. (See Solomon Edun's Challenges and Opportunities in Africa available here, but also see the African Union Commission, The Digital Transformation Strategy for Africa (2020–2030) (2020).

[40] Robinson, N., Kask, L., & Krimmer, R. (2019). The Estonian data embassy and the applicability of the Vienna Convention: An exploratory analysis. In *Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance* (pp. 391–396). ACM. https://doi.org/

[41] Robinson, Kask and Krimmer.

[42] Musoni et al., Global Approaches to Digital Sovereignty, Discussion Paper No. 344 (2023).

[43] Ministry of Electronics and Information Technology. (2022). National Data Governance Framework Policy (Draft). https://www.thehinducentre.com/resources/67557000-National-Data-Governance-Framework-Policy_compressed.pdf.

[44] D.Ojha, DSCI. (n.d.). Data Security Council of India. https://www.dsci.in/dsci-blog/content/data-embassies-legal-and-technological-implications-india .

[45] African Union, 2022.

[46] Centre for the Fourth Industrial Revolution (C4IR). (n.d.). Centre for the Fourth Industrial Revolution (C4IR). http://c4ir.rw/

[47] Xalam Frontiers Market. (2024). *Xalam Africa Data Center Report 2024: Client sampler and table of contents*. African Data Centres Association. https://africadca.org/wp-content/uploads/2024/07/Xalam-Africa-Data-Center-Report-2024-Client-Sampler-and-ToC.pdf

[47] Miao, C. (2025, July 2). Africa data centres power up. Energy News Network. https://energy-news-network.com/industry-news/africa-data-centres-power-up/

[48] International Energy Agency. (2022). Africa Energy Outlook 2022: Key findings. https://www.iea.org/reports/africa-energy-outlook-2022/key-findings.

[49] Thomas, D. (2025, March 24). Cassava and Nvidia to launch Africa's 'first AI factory' African Business. https://african.business/2025/03/technology-information/cassava-and-nvidia-to-launch-africas-first-ai-factory

[50] Higgins, A. (2025, March 24). Cassava to upgrade its data centres with NVIDIA supercomputers to drive Africa's AI future. - Cassava Tech. Cassava Tech. https://www.cassavatechnologies.com/cassava-to-upgrade-its-data-centres-with-nvidia-supercomputers-to-drive-africas-ai-future/

[51] Markets, R. A. (2025, June 23). Middle East & Africa Existing & Upcoming Data Center Database 2025: Over $15.5 billion in new investments to fuel data center growth in MEA by 2027. GlobeNewswire News Room. https://www.globenewswire.com/news-release/2025/06/23/3103576/28124/en/Middle-East-Africa-Existing-Upcoming-Data-Center-Database-2025-Over-15-5-Billion-in-New-Investments-to-Fuel-Data-Center-Growth-in-MEA-by-2027.html

[52] Nwenyi, O. (2025, March 11). Why Africa needs local cloud providers like Nebula. Nebula Blog. https://blog.usenebula.io/why-africa-needs-local-cloud-providers-like-nebula/.

[53] Obi, U. (2024, October 17). Redefining Data Sovereignty: How Nigeria's local cloud providers are driving cost-efficient solutions - Businessday NG. Businessday NG. https://businessday.ng/news/legal-business/article/redefining-data-sovereignty-how-nigerias-local-cloud-providers-are-driving-cost-efficient-solutions/

[54] Blessing, O., & Blessing, O. (2025, January 16). *Amazon Web service introduces Naira payments to lower cloud costs for Nigerian businesses*. MSME Africa. https://msmeafricaonline.com/amazon-web-service-introduces-naira-payments-to-lower-cloud-costs-for-nigerian-businesses/

[55] Open Access Data Centres. (2024, February 29). Africa's potential as a cloud solutions provider. https://openaccessdc.net/africas-potential-as-a-cloud-solutions-provider/

[56] U.S. Congress. (2018). Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348. https://www.congress.gov/bill/115th-congress/house-bill/4943 , Microsoft Corp. v. United States, 584 U.S. ___ (2018).

[57] Navigating digital sovereignty in Africa:A review of key challenges and constraints - ACRP. (n.d.). https://africachinareporting.com/navigating-digital-sovereignty-in-africa-a-review-of-key-challenges-and-constraints/

[58] The global foreign exchange market in a higher-volatility environment. (n.d.). https://www.bis.org/publ/qtrpdf/r_qt2212f.htm

[59] Okamgba, J. (2025, April 28). FX crisis slows Nigeria's data centre investments. Punch Newspapers. https://punchng.com/fx-crisis-slows-nigerias-data-centre-investments/

[60] Harrisberg, K., & Mensah, K. (2022, June 21). As young Africans push to be online, data cost stands in the way. World Economic Forum. https://www.weforum.org/stories/2022/06/as-young-africans-push-to-be-online-data-cost-stands-in-the-way/

[61] Africa's data centre challenge. (n.d.). https://abmagazine.accaglobal.com/global/articles/2025/feb/business/africa-s-data-centre-challenge.html

[62] Venske, T. (2023). Navigating digital sovereignty in Africa: A review of key challenges and constraints. The Africa Governance Papers, 1(4). https://tagp.gga.org/index.php/system/article/view/51

[63] Gooding, M. (2024, May 22). Microsoft and G42 to build geothermal-powered data center in Kenya. Data Center Dynamics. https://www.datacenterdynamics.com/en/news/microsoft-and-g42-to-build-geothermal-powered-data-center-in-kenya.

[64] ResearchAndMarkets.com. (2025, June 18). *Kenya Colocation Data Center Portfolio Analysis Report 2025: Detailed Analysis of 13 Existing Data Centers and 9 Upcoming Data Centers*. Business Wire. https://www.businesswire.com/news/home/20250618339125/en/Kenya-Colocation-Data-Center-Portfolio-Analysis-Report-2025-Detailed-Analysis-of-13-Existing-Data-Centers-and-9-Upcoming-Data-Centers---ResearchAndMarkets.com

[65] ResearchAndMarkets.com (2025, June 18).

[72] Nyabola, C. T. N. (2019, November 5). Nanjala Nyabola on the "Digital Colonialism" transforming Kenya's political discourse. Centre for International Governance Innovation. https://www.cigionline.org/articles/nanjala-nyabola-digital-colonialism-transforming-kenyas-political-discourse/

[66] Lewis, S. (2024, April 2). Unveiling the Invisible: A closer look at data center risk avoidance strategies. EkkoSense. https://www.ekkosense.com/resources/industry-insight/unveiling-the-invisible-a-closer-look-at-data-center-risk-avoidance-strategies/ .

[67] Amin, M. (2025, March 5). Rebuilding Sudan's digital infrastructure amidst conflict. VoxDev. https://voxdev.org/topic/institutions-political-economy/rebuilding-sudans-digital-infrastructure-amidst-conflict

[68] Internet Society. (n.d.). Internet crossing borders: Boosting the Internet in Landlocked Developing Countries. https://www.internetsociety.org/wp-content/uploads/2017/10/LLDC_ExecSummary_20171004.pdf .

[69] Klymash, M., Demydov, I., & Baydoun, N. A. (2019). The "Data Embassies" concept as a secure communication core for e-Gov implementation in emerging states. In Proceedings of the 2019 IEEE 20th International Conference on Computational Problems of Electrical Engineering (CPEE) (pp. 1–4). IEEE. https://doi.org/10.1109/CPEE47179.2019.8949152.

[70] *Africa's data centre growth opportunity*. (n.d.). https://aiimafrica.com/media/media-centre/africas-data-centre-growth-opportunity/ .

[71] United Nations. (n.d.). Global Digital Compact. In A/79/L.2 (pp. 24–15616). https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf .

[72] Experts urge for mandatory reporting of AI data centers' energy & water use amid environmental concerns - Business & Human Rights Resource Centre. (2025, February 7). Business & Human Rights Resource Centre. https://www.business-humanrights.org/en/latest-news/experts-urge-for-mandatory-reporting-of-ai-data-centers-energy-water-use-amid-environmental-concerns/ .

[73] *Tackling Tech: The Need for Environmental Accountability and Regulation to Protect the Planet and its People | Heinrich Böll Stiftung | Washington, DC Office - USA, Canada, Global Dialogue*. (2024, September 9). Heinrich Böll Stiftung | Washington, DC Office - USA, Canada, Global Dialogue. https://us.boell.org/en/2024/09/09/tackling-tech-need-environmental-accountability-and-regulation-protect-planet-and-its .

[74] African Development Bank. (2024, May 17). Congo: New data centre funded by African Development Bank will cement national and subregional digital sovereignty. African Development Bank. https://www.afdb.org/en/news-and-events/congo-new-data-centre-funded-african-development-bank-will-cement-national-and-subregional-digital-sovereignty-70847.

[75] African Development Bank, 'Congo: New Data Centre.' (2024, May 17).

[83] BTI 2024: Congo, DR. (2024 March). BTI 2024. https://bti-project.org/en/reports/country-dashboard/COD

[76] Olanrewaju, D. (2025, June 19). Nigeria's data center growth prospects amid power constraints. https://www.connectingafrica.com/data-centers/nigeria-s-data-center-growth-prospects-amid-power-constraints .

[77] Okamgba, J. (2025a, March 28). *Broadband, data centre gaps threaten $1tn economy goal - Telcos*. Punch Newspapers. https://punchng.com/broadband-data-centre-gaps-threaten-1tn-economy-goal-telcos/

[78] Jaiyeola, T. (2024, September 9). Rising energy costs hamper data center growth in Nigeria - Businessday NG. Businessday NG. https://businessday.ng/technology/article/rising-energy-costs-hamper-data-center-growth-in-nigeria/

[79] Okamgba, J. (2025, April 1). Rack Centre powers new data hub with natural gas. Punch Newspapers. https://punchng.com/rack-centre-powers-new-data-hub-with-natural-gas/ .

[80] Miao, C. (2025, July 2). Africa data centres power up. Energy News Network. https://energy-news-network.com/industry-news/africa-data-centres-power-up/ .

[81] Soulé, F. (2024). Digital Sovereignty in Africa: Moving beyond Local Data Ownership. In Policy Brief No. 185, June 2024. https://www.cigionline.org/static/documents/PB_no.185.pdf.

[82] Robinson, Kask and Krimmer.

[83] Estonia–Luxembourg Data Embassy Agreement (n 14)

[84] Robinson, Kask and Krimmer (n 30).

[85] Robinson, Kask and Krimmer (n 30).

[86] Robinson, Kask and Krimmer (n 30).

[87] VCDR, 1961.

[88] Berchtold, J. (2025, April 25). A new framework for data embassies: Saudi Arabia's Global AI Hub Law (via Passle). Passle. https://viewpoints.reedsmith.com/post/102k9af/a-new-framework-for-data-embassies-saudi-arabias-global-ai-hub-law .

[89] Mudric, M. (2025, March 31). Data embassies: Protecting nations in the cloud - Diplo. Diplo. https://www.diplomacy.edu/blog/data-embassies-protecting-nations-in-the-cloud/ .

[90] St Emmanuel, S. A. (2023, April 5). State responsibility and inviolability of diplomatic premises under international law: The case of the attack on the Nigerian High Commission in Accra, Ghana. Ajayi Crowther University Law Journal. https://aculj.acu.edu.ng/index.php/lj/article/view/42/40.

[91] The Iranian hostage crisis - Short history - Department History - Office of the Historian. (n.d.). https://history.state.gov/departmenthistory/short-history/iraniancrises .

[92] ABC News. (2024, April 6). Ecuadorian police raid Mexican embassy to arrest former vice-president Jorge Glas. https://www.abc.net.au/news/2024-04-06/ecuadorian-police-raid-mexican-embassy-to-arrest-jorge-glas/103678028

[93] African Leadership Magazine (n 4).

[94] Admin. (2025, February 25). Data centers: which African countries offer the best opportunities? Extensia Ltd. https://extensia.tech/data-centers-which-african-countries-offer-the-best-opportunities/ .

[95] Benamara, A. (2025, February 27). EXCLUSIVE Q&A: Africa's blueprint for a secure digital future. TechAfrica News. https://techafricanews.com/2025/02/27/exclusive-qa-africas-blueprint-for-a-secure-digital-future/ .

[96] *Navigating digital sovereignty in Africa:A review of key challenges and constraints - ACRP*. (n.d.-b). https://africachinareporting.com/navigating-digital-sovereignty-in-africaa-review-of-key-challenges-and-constraints/

[97] Shankar IAS Parliament '(n 42)' (5 April 2024). Accessed 14 June 2025, https://www.shankariasparliament.com/blogs/pdf/data-embassies .

[98] Saaia-Admin. (2025, April 8). Africa Declaration on Artificial Intelligence. SAAIA. https://saaiassociation.co.za/africa-declaration-on-artificial-intelligence/