Assessing the Suitability of the African Union Data Policy Framework for Digital Trade in Africa:

A South African Customs Union (SACU) Case Study

Shamira Ahmed

White Paper

DepHUB
Data Economy Policy Hub

CIPESA

Table of Contents

Acknowledgements

The research was funded by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA) as part of its multi-country research project, ***Catalysing Good Data Governance Policy and Practice in Africa***, that seeks to advance progressive data governance policy and practice at continental and national level through research, stakeholder engagement and network building.

Executive Summary

In the 21st century, digital trade has become a cornerstone of global free trade, offering significant opportunities for economic growth and development across Africa. As African countries and regional economic communities (RECs) embrace digital transformation, coherent data governance frameworks are essential to harness the potential of the data economy.

However, the transition towards the data economy raises critical policy challenges, including data privacy, cybersecurity, the digital divide, and data sovereignty. These challenges intersect with broader issues of national security, geopolitical tensions, and emerging technologies such as artificial intelligence (AI).

In the context of Africa's digital transformation, the African Union's (AU) Data Policy Framework (DPF) represents a major step toward ensuring data sovereignty and addressing continent-wide concerns. However, the DPF is not fully adequate for fostering a Digital Single Market, cross-border data flows (CBDF), digital trade, and e-commerce across the Southern African Customs Union (SACU) member states—South Africa, Botswana, Namibia, Eswatini, and Lesotho—or across Africa in general. Amongst other shortcoming's the DPF's reliance on national data protection authorities to lead data governance risks creating fragmented regulations, which conflict with the transnational nature of digital technologies and data.

While the DPF emphasizes legal frameworks, it lacks the necessary enforceable transversal approach to enhance regional collaboration and harmonization required to build trustworthy, efficient regional data ecosystems. This absence of a transversal coordinated regional approach risks increasing regulatory complexity, creating barriers to trade, and stifling the growth of e-commerce and digital trade. Furthermore, tackling the risks associated with privacy, security, and the digital divide demands a formally binding coordinated regional strategy, something the DPF's current design does not adequately support.

To fully capitalize on the potential of digital technologies for economic growth, SACU countries need a more harmonized and collaborative approach to data governance. The Digital Protocols of the Africa Continental Free Trade Area (AfCFTA) offer a more appropriate pathway, supporting cross-border data flows and driving digital trade across the continent. A proactive sociotechnical approach, which better addresses the complexity of the data economy, must be adopted to balance the risks and benefits of digital transformation.

To overcome multidimensional barriers, SACU member states must adopt a transversal approach that aligns digital trade policies with broader economic, regulatory, and infrastructure goals. A transversal approach requires a much-needed focus on both supply-side policies, such as enhancing digital infrastructure, and demand-side policies, such as promoting digital capabilities.

1. Introduction

In the 21st century, digital trade is a fundamental component of free trade and essential for enhancing intra-African trade through potentially unprecedented opportunities for economic growth and development (UNCTAD, 2023) Digital trade and global data governance are at a unique crossroads, raising significant policy challenges that influence a country's ability to adapt, adopt, and use frontier technologies (UNCTAD, 2021a), these challenges include data privacy, cybersecurity, public access to data, the digital divide, data sovereignty, and antitrust, to name a few.

The governance of digital trade and cross-border data flows highlights significant challenges for both international cooperation and domestic regulation (Aaronson & Leblond, 2018). Government measures that prohibit or impede international data transfers are also increasing in response to shifting national economic policy priorities, rising geopolitical tensions, national security concerns, and the effect of emerging technologies like artificial intelligence (AI) (Schweitzer et al.,2024; Ahmed, 2023b).

The volume and value of cross-border data flows have grown exponentially in recent years, driven by the rapid expansion of the data economy (UNCTAD, 2021b). Worldwide, various regional trade blocs are increasingly leveraging trade agreements to address digital trade and cross-border data flows by including provisions on digital trade, data flows, and data localization (Burri et al., 2024).

As many African countries and regional economic communities (RECs) begin to embrace digital transformation and integration including through trade-related instruments, it is crucial to establish coherent data governance frameworks that ensure privacy, security, and equitable distribution of benefits from the data-driven data economy (ECOWAS, 2024; Ahmed, 2023a). Furthermore, continental agreements such as the Draft Protocol to the African Continental Free Trade Area on Digital Trade (the Protocol), if designed, adopted, and operationalised well, could contribute to the realisation of a digital single market (DSM).

However, the successful integration of digital trade within the African context relies on the effectiveness and harmonization of various prerequisites and enablers, such as cross-border data policy frameworks and essential network infrastructure, among others. (UNCTAD, 2023; Abrahams et al., 2023). Despite initiatives and attempts to harmonise certain governance aspects related to cross-border data through the Convention on Cyber Security and Personal Data Protection (Malabo Convention) (AU, 2014), the Protocol, the Policy and Regulatory Initiative for Digital Africa (PRIDA) (PRIDA, 2024), and the Africa Union Digital Transformation Strategy for Africa (DTS) (2020–2030) (AU, 2020), the challenges in creating a robust unified approach to cross border data governance are still significant, and considerable implementation work remains.

The African Union (AU) Data Policy Framework (DPF), endorsed in February 2022, outlines a comprehensive set of principles and guidelines for data governance, data protection, data value creation, and data-driven innovation across the Continent (AU, 2022). The DPF covers a wide range of issues, including data sovereignty, data sharing, data security, and digital infrastructure development, to name a few. The DPF is intended to facilitate the growth of Africa's data economy, including promoting the seamless flow of data across African borders. The DPF is intended to complement other existing regional integration policy documents and similar initiatives that are developed to guide AU Member States in building robust national data ecosystems and capabilities, to ensure that countries can effectively harness the value of data generated by citizens, government entities, and industries.

The South African Customs Union (SACU), comprising South Africa, Botswana, Lesotho, Namibia, and Eswatini, is a well-established economic bloc with a long history of trade integration amongst its Member States (SACU, 2024). However, SACU's digital landscape is still evolving, with varying levels of

endowments, capabilities, and enablers such as digital infrastructure, robust data governance policies, and regulatory frameworks amongst the SACU member states.

Practical international and regional frameworks that support cross border data flows (CBDF) are crucial for establishing a unified equitable African DSM and advancing continental development goals through e-commerce, e-payments, and digital trade (Ahmed, 2023b; Beyleveld & Sucker, 2023).

Given the importance of CBDF for digital trade and overall digital transformation, it is crucial to assess the suitability of the DPF for fostering digital trade within an established REC, such as SACU. SACU serves as a focal case study, given its significant role in regional trade, its well-established physical trade integration, its common negotiating mechanism, and the potential of its common tariff schedule (SACU, 2024; Abrahams et al.,2023).

While there are ongoing initiatives piloted by RECS such as the Internet and digitally enabled services in Eastern and Southern Africa (IDEA), implemented by the Common Market for Eastern and Southern Africa (COMESA), and the Economic Community of West African States's (ECOWAS) regional e-commerce strategy, there is limited research on CBDF from a digital trade lens in existing African RECs. Assessing the suitability of DPF within the SACU context can provide valuable insights into the DPF's potential to address the region's unique cross-border data governance challenges and opportunities to facilitate digital trade at a continental level and globally.

This paper evaluates the suitability of the DPF for facilitating the complex multidimensional aspects of digital trade amongst SACU member states. The aim of this paper is to provide a better understanding of the transnational changes shaping digital trade with a view to informing how these might be reflected in holistic policy design and implementation in the African context.

2. Background

2.1. Digital transformation, digital trade, and digital inequality

Digital transformation is a phenomenon that highlights the influence of digital technologies and data on both existing and new societal, political, financial, and industrial activities. This phenomenon is rapidly progressing globally, impacting all sectors —Digital transformation, spurred by digitalisation, data, and data-intensive frontier technologies, has contributed to the transformation of international trade in goods and services (digital trade) and transformed the way economy's function, creating new opportunities while also presenting ethical, legal, societal and policy challenges that require trusted and equitable flow of capital, goods, knowledge, services, and people (UNCTAD 2021b; Ciuriak & Ptaškina, 2018).

Enhanced use of digital technologies across Africa is projected to increase digital services exports by USD$74 billion between 2023 and 2040, effectively doubling the continent's global market share (REF). Improved digital connectivity, combined with a supportive regulatory environment, could reduce trade costs by up to 25 percent (UNCTAD, 2023). Additionally, digitally delivered services (DDS) offer a means to overcome challenges by reducing information asymmetry and facilitating direct connections between suppliers and customers, digital trade promotes inclusiveness, particularly benefiting groups that are often marginalised on traditional cross-border trade micro, small & medium enterprises (MSMEs), women, and youth (UNCTAD, 2023). While digital trade holds significant potential to drive economic growth and development in Africa, if governed inadequately the movement of digital goods and services across borders also carries the risk of deepening existing multidimensional inequalities and exclusions, including unequal concentration of resources and increased socioeconomic instability (UNCTAD,

2021a). As with past technological revolutions, the benefits of leveraging frontier technologies to enhance trade can be immense, but they will not be realized without deliberate and strategic interventions (UNCTAD, 2021b).

Furthermore, there is increased complexity in governing global rules and norms for digital cooperation through trade since the digital trade agenda now encompasses a mix of traditional trade topics, such as trade facilitation, alongside a range of rapidly evolving digital policy issues (Aaronson, 2018; Ciuriak & Ptaškina), including, but not limited to:

i. Cross-border data flows and data localization
ii. E-signatures and authentication
iii. Network neutrality
iv. Online consumer protection and privacy
v. Unsolicited commercial electronic messages (spam)
vi. Open government data
vii. Customs duties on electronic transmissions
viii. Cybersecurity
ix. Access to the source code of computer programs
x. E-payments

Given the patchwork of proposals and initiatives, it is likely that the net outcome of proposed frameworks will require multistakeholder transnational governance to build the capabilities countries need to take advantage of the rapid expansion of the data economy, enabled by technologies such as AI, cloud computing, and autonomous vehicles, which has created new opportunities for businesses to engage in cross-border trade of goods and DDS (UNCTAD, 2023)..

However, there is a significant data divide between high income and low-income countries reflected by their ability to access, collect, integrate, store, analyse, and utilise data to create commercial and public value (UNCTAD, 2021a). The digital divide is particularly pronounced in the world's least developed countries (LDCs), landlocked developing countries (LLDCs), and small island developing states (SIDS) (Rattray,2024; UNDP,2024). As the continent with the highest number of LDCs and LLDCs, the digital divide across Africa remains an ongoing concern, most recent data from the International Telecommunication Union (ITU) for 2023 indicates that vulnerable countries, particularly LDCs, face significant challenges in Internet accessibility, usage, and penetration, on average, only 19 percent of the population using the Internet in LDCs, while LLDCs report an average Internet usage rate of approximately 27 percent average usage rates that are below the global average of 67 percent (ITU, 2023).

Both LDCs and LLDCs experience considerably lower Internet penetration rates than the average of nearly 90 percent Internet penetration seen in more wealthier countries (ITU, 2023). Many people in LDCs and LLDCs also have limited Internet access, the low levels of Internet access need a coordinated collaborative and urgent solution, Internet access is a vital driver of technological innovation and economic growth (Xiao et al., 2024), the disparity on access to Internet in Africa is concerning, particularly since there are 33 LDCs[1] out of 54 countries across that are characterised by low income, political instability, weak socioeconomic and environmental resilience, inadequate critical infrastructure, and low labour market absorption rates (UNCTAD 2021c).

The global digital divide threatens to further weaken the position of many low and middle income (LMICs) in many global value chains (GVCs), as firms from high income countries (HICs) dominate the

[1] Sub-Sahara Africa is the continent with has the highest number of LDC's in the world.

development of new digital technologies including reaping the benefits of first-mover advantage and network effects, which are often exacerbated by a wide range of issues (UNCTAD, 2019).

2.2. The multilateral trade system and cross-border data flows

For decades, the multilateral trade system (MTS) has played a crucial role in facilitating cross-border data flows, which are essential for global economic integration and the data economy (Ciuriak & Ptaškina, 2018). The MTS, consisting of international trade agreements (ITAs) and frameworks that govern the exchange of digital goods, DDS, and data across borders, has been at the forefront of international data governance through the operationalisation of the first binding international rules related to digital trade (Burri et al., 2024). Despite their shortcomings (UNCTAD,2020), multilateral organisations such as the World Trade Organization (WTO) and the World Intellectual Property Organization (WIPO) have offered an established fora for improving data governance and for the protection of intellectual property rights (IPRs), which attempt to balance approaches to a wide range of issues such as access to data , fostering generation of data, and protecting legitimate interests in the trade context (Burri et al., 2024).

However, the data economy creates new challenges that has resulted in a fragmented digital trade landscape (Casalini & González, 2019). Furthermore, countries and regions with geopolitical heft such as the United States of America (USA), the European Union (EU), and China each have distinct approaches to data governance, which create geopolitical rifts that exacerbate digital divides and perpetuate uneven geopolitical power dynamics where they (USA, EU, and China) are essentially the three data standard makers and other countries and regions are rule takers (Ahmed et al., 2023). These geopolitical power dynamics combined with unilateral influence to operationalise approaches to data governance raise significant implications for the governance of CBDF, which presents both challenges and opportunities for institutions like the WTO in harmonising regulation to govern the movement of data (Aaronson & Leblond, 2018).

The governance of digital trade and CBDF highlights significant challenges in both international cooperation and domestic regulation as countries navigate the complexities of digital trade. The interplay between international commitments and national interests will continue to influence regulatory approaches and the broader dynamics of global trade spanning AI, other emerging technologies, semiconductors, or CBDF— to guide digital trade policymaking (WTO, 2024). Recent developments, such as the extended suspension of customs duties on electronic transmissions until March 31, 2026, and the push for liberalized e-commerce rules led by the Global North, can obscure the complexities and potential risks associated with such policies, particularly for developing countries (UNCTAD, 2020).

Progress has been slow due to the fundamental cultural, equity, and policy divergencies among countries (UNCTAD, 2020). Both the WTO and WIPO have faced challenges in adapting their frameworks to the rapidly evolving data economy and the complexities of data governance in addressing CBDF and digital trade issues (Burri, 2017).

Furthermore, the existing approach to managing CBDF through trade agreements has not resulted in binding, universal, or interoperable rules governing data usage since trade negotiations have traditionally focused on removing restrictions to international trade but are not suitable for addressing issues of regulatory convergence (Burri et al., 2024). Progress toward harmonization for the necessary regulatory safeguards of data rights, or common data standards and architectures that enable the exchange of

information, could benefit from more cooperative and nonbinding approaches offered by international instruments in other related sectors (Aaronson, 2017).

Beyond being underrepresented in digital trade talks, the fragmented nature of global governance for digital trade and CBDF presents significant challenges for African countries (Pittet, 2022). The ongoing discussions on e-commerce at the WTO also highlight the urgency of establishing coherent policies that balance the need for data mobility with essential protections for privacy and security (UNCTAD, 2020).

2.3. Why cross-border data flows matter for digital trade

Data is fundamentally different from traditional goods and services, data's non-scarcity, role in enabling digital services, facilitation of global value chains, and contribution to innovation underscore its importance in the modern global data-driven data economy. Data is ubiquitous, exists in various formats—from structured, numeric data in traditional databases to unstructured forms like text documents, emails, videos, and financial transactions (Aaronson, 2018). Digital trade and CBDF are closely intertwined, CBDF enables the transfer of data, information, and digital content across national borders, which is necessary for the functioning of digital trade platforms and services (OECD et al., 2019). Examples of CBDF include, but are not limited to:

i. Transmitting customer data for online purchases
ii. Sharing business information and data between subsidiaries
iii. Storing and processing data in cloud computing services
iv. Enabling digital services like online banking, streaming, and software as a service (SaaS)

Services such as cloud computing, e-commerce, and digital communications rely heavily on the ability to move data seamlessly across borders. Companies, governments, and individuals are leveraging data to develop new DDS, including apps, AI, and the Internet of Things (IoT), which offer immense opportunities for enhancing productivity, scientific discovery, climate change mitigation, public service delivery, innovative business models, remote work, education, and healthcare. These data-driven services depend on extensive data pools and the relatively unrestricted flow of data across borders, facing few market access or governance barriers (UNCTAD 2021a).

As more data flows across borders, concerns about its use and misuse have emerged (Casalini & González, 2019), resulting in varying national regulations, which can create friction and inefficiencies. For instance, regulations aimed at protecting personal data or ensuring national security can restrict data movement, impacting businesses that rely on global data access. Therefore, establishing interoperability is crucial for maximizing the benefits of CBDF for facilitating digital transformation, enabling businesses to operate effectively in a globalized economy and contributing to societal benefits (UNCTAD 2021a).

2.4. Cross border data flows and Internet governance

Outside the auspices of trade policy discussions, governments, businesses, academia, and civil society have spent the past twenty years arguing over the jurisdiction that should apply when information travels across the globe, and what common rules should remain. Data governance, together with rules on access to information, are some of the key components of mitigating internet fragmentation (Drake et al., 2016).

Net neutrality, digital market access, data localization, privacy, and competition are among the many regulatory issues emerging as digital transformation reshapes international trade (Ciuriak & Ptaškina, 2018). The shift of data governance discussions to the realm of trade does not immediately solve the entrenched conflicts between the promise of the internet to connect humanity by bringing universal access to information on the one hand and the priorities of governments and powerful private actors from countries with geopolitical heft (UNCTAD, 2021a). The potential for rules and policies over data to influence trade adds a new layer of complexity to existing internet governance discussions framed under the prisms of human rights, national security, economic development, or broader geopolitical debates.

Coordinated and coherent international efforts to promote technical standards for data protection and cybersecurity are essential to ensure interoperability and the ongoing discussions about data and internet governance are crucial for shaping a global data economy that is fair, secure, and accessible to all (Casalini & González, 2019).

However, the wide range of stakeholders and states implicated by current rules and the various initiatives at play may make it challenging to achieve significant outcomes on a global level (Drake et al., 2016).

3. Critiquing the African Union Data Policy Framework: A digital trade perspective

Digital trade often encounters non-tariff barriers that can impede the movement of digital goods and services. These barriers can include customs procedures and approaches to data governance that are not adapted for digital transactions across borders, leading to delays and increased costs (Ciuriak & Ptaškina, 2018; Drake et al., 2016).

Governing CBDF is a complex challenge that requires careful consideration to ensure that data can move freely across border while protecting privacy, security, and socioeconomic interests. Analysis of existing literature reveals that the CBDF and digital trade should be guided by principles that prioritize trust, interoperability, proportionality, transparency, economic considerations, international cooperation, and inclusivity, to name a few (González, 2021).

Despite the commendable provisions of the DPF, unlike the Malabo Convention or African Continental Free Trade Agreement (AfCFTA), the DPF functions only as a guiding framework rather than a legally binding instrument subject to ratification. The DPF does not have a legally binding effect on member states (MS) but provides very broad guidelines on how MS can approach and attempt to harmonise data governance at a continental level. Critiquing the DPF from a digital trade lens is essential for several reasons: the DPF does not provide detailed guidelines for data governance beyond privacy and data protection, which can lead to inconsistent implementation across member states, hindering the potential interoperable free and secure flow of data across the continent.

The DPF outlines approaches to data governance from an African lens while addressing the complexities of various aspects such as privacy, cybersecurity, and data value creation, amongst others, in Africa (AU 2022).

The critiques regarding three main categories: scope, implementation, and approach from a digital trade perspective are as follows:

3.1. Approach

3.1.1. Data sovereignty and cross-border data flows

The DPF aims to facilitate CBDF while safeguarding human rights and data protection through the creation of a conducive environment for data sharing to bolster intra-African trade and digital innovation to support the DSM (AU, 2022). Simultaneously, the DPF emphasises data sovereignty (AU, 2022), at national and continental levels which if designed inadequately can lead to stringent data localization requirements, that essentially perpetuate a fragmented approach to governing data amongst African countries (Soule, 2024). The emphasis on data sovereignty presents a double-edged sword: while it aims to empower African nations to govern their data in alignment with local laws and values, inadequate design of these frameworks can lead to stringent data localization requirements, which, in turn, risks perpetuating a fragmented approach to data governance across the continent.

If designed inadequately data sovereignty could significantly impacts digital trade and CBDF in various ways, influencing how countries approach data governance and international commerce, with unintended negative consequences (Aaronson, 2021; Dabrock et al., 2021). For example, South Africa has implemented the Protection of Personal Information Act (POPIA) and recently introduced the National Policy on Data and Cloud. These regulations aim to ensure that personal data generated within the country remains under local control. However, such stringent localization requirements can create barriers for businesses that operate across borders, complicating compliance and potentially stifling digital trade. As highlighted in a report by Nkala and Maswabi (2022), while these laws are designed to protect citizens' privacy and enhance national security, they can inadvertently limit the ability of companies to share data efficiently with regional partners or global markets.

Similarly, Nigeria's Data Protection Regulation (NDPR) reflects a growing trend among African nations to impose data localization policies as a means of fostering economic development and protecting citizen privacy. However, as noted by Peltola (2023), these measures can also lead to increased operational costs for businesses that must navigate varying regulations across different jurisdictions. The potential for regulatory fragmentation may deter foreign investment and hinder local startups from scaling their operations effectively. If not designed adequately, such approaches to data sovereignty could significantly impact digital trade and CBDF. Countries may find themselves isolated in their regulatory environments, making it challenging to engage in international commerce and collaborate on technological advancements. The unintended consequences of fragmented national data governance could ultimately undermine the very objectives that the DPF seeks to achieve—namely, fostering a cohesive DSM that promotes economic growth and innovation across Africa.

Another major challenge is the tension between national sovereignty and the global nature of the Internet, CBDF, and digital trade (Gao, 2021). Balancing the legitimate interests of states in regulating data flows to maintain their sovereignty with the need for interoperability, innovation, and collaboration on a global scale requires careful collaboration, coordination, and cooperation among stakeholders (IS, 2022). The fragmentation of regulations across different jurisdictions under the rationale of data sovereignty can create legal and compliance burdens as well as hinder the competitiveness of businesses operating in global markets (Hummel et al., 2018).

A incoherent continental regulatory landscape creates challenges and opportunities for large multinational companies (MNCs) —large MNCs face an unpredictable landscape that may hinder the potential scaled benefits of regional investments, perpetuating the uneven development between countries, alternatively, large MNCs can navigate the uneven regulatory landscape by leveraging regulatory arbitrage, at the detriment of collective regional growth. Beyond large MNCs, an incoherent

continental data regulatory landscape can also exacerbate information asymmetries for cross border micro-small and medium enterprises (MSMEs).

The balance between promoting data flows and enforcing data protection remains delicate, the DPF's approach to data localization—advocating for limited localization while promoting broader data flows—could lead to tensions among AU MS. Countries may still adopt restrictive measures under the rationale of protecting human rights, maintaining social stability, or protecting national security, which could undermine the framework's goal of enhancing cross-border data transfers and facilitating the DSM. While the DPF encourages cooperation among member states, the inherent culture of secrecy and national sovereignty concerns prevalent in many African countries could hinder efforts to achieve true interoperability (Hlomani & Ncube, 2022). Countries may prioritize their own data governance regulations over collaborative initiatives, potentially stalling progress toward a unified data ecosystem that supports the DSM.

As an alternative, the concept of "Data Flow with Data Rights" goes beyond the "Data Free Flow with Trust" (DFFT)[2] Framework to include economic rights to data (IT, 2022). While there are several advantages of DFFT over a strict data sovereignty approach such as interoperability, balancing interests, encouraging cooperation, providing flexibility, and supporting economic development.

However, for developing countries, the DFFT framework could exacerbate economic exploitation and wealth concentration due to their limited influence in global discussions on CBDF. There are also concerns that DFFT could facilitate the extraction of data without fair compensation or benefits to the local population, which could lead to a form of "data colonialism," where developing countries become mere exporters of raw data without gaining economic value from it due to weak endowments and enablers to create value from data (Couldry & Mejias, 2019). Lastly, developing countries often face significant challenges in terms of technological infrastructure and capacity. The DFFT framework assumes a level of digital readiness and capability that many developing nations may not possess. Without adequate infrastructure to support data flows, such as reliable internet connectivity and data storage facilities, these countries may struggle to fully participate in the benefits of DFFT.

3.1.2. Advocacy for regulatory sandboxes

The DPF advocates for regulatory sandboxes, which in ideal contexts (Appaya et al., 2020), are designed to foster innovation by allowing startups and fintech companies to test their products and services in a controlled environment with regulatory oversight (AU, 2022).

However, according to the World Bank, the maturity of the existing ecosystem is crucial to ensure the effectiveness and implementation of a sandbox. In a nascent market, a sandbox may not be cost efficient for regulators, as sandboxes are resource intensive and bear large opportunity costs (Appaya et al., 2020). There are also issues with compliance and legitimacy, including ensuring trust, accountability, responsive enforcement, the politics of participation, and post-sandbox oversight, recorded in HIC ecosystems (Johnson, 2023) that will most likely be prevalent in LMICs.

Furthermore, without feasibility assessments before setting up any sandbox initiative—particularly in developing countries, sandboxes may result in detrimental effects and potential "Risk washing" (Brown & Piroska, 2022). Most of the literature and practice on regulatory sandboxes is primarily from the fintech sector and mainly from ecosystems with more digital technology maturity, which highlights that LMICs may require the requisite maturity, enablers, endowments, and conditions before diving into the creation

[2] The concept of Data Free Flow with Trust (DFFT) aims to promote the free flow of data while ensuring trust in privacy, security, and intellectual property rights. https://www.digital.go.jp/en/dfft-en/

of a sandbox (Appaya et al, 2020). Furthermore, many LMICs face significant resource limitations, including insufficient funding, inadequate infrastructure, and a lack of skilled personnel to successfully implement and maintain regulatory sandboxes (Appaya et al., 2020). As a result, sandboxes may struggle to provide adequate support and oversight, leading to ineffective regulation and increased risks for consumers (Wechsler et al., 2018). There are also risks of regulatory capture, where established players influence the sandbox to maintain their competitive advantages at the expense of new entrants, which creates an uneven playing field where only well-connected firms gain access to the sandbox, stifling competition and innovation. In LMICs an uneven playing field can exacerbate existing inequalities and limit opportunities for smaller, less-resourced startups (Appaya et al., 2020).

Regulatory sandboxes may offer temporary relief from regulatory burdens (for a few), they fail to address the underlying systemic issues that hinder innovation in many countries. For instance, outdated regulations or a lack of coherent digital strategies mean that startups often encounter the same challenges once they exit the sandbox, resulting in a cycle of dependency without meaningful progress. Critics argue that sandboxes can be misused, becoming exclusive spaces for well-connected firms, which reinforces existing power dynamics and perpetuates systemic inequalities (Appaya et al., 2020).

Regulatory sandboxes often are geared towards short-term experimentation rather than long-term regulatory frameworks. This short-sightedness can hinder the development of comprehensive policies that address the broader implications of emerging technologies. In developing countries, where long-term agile and anticipatory planning is essential for sustainable growth, short-sightedness can stifle innovation and economic development (Wechsler et al., 2018).

While regulatory sandboxes have gained popularity as a mechanism for fostering data economy innovation in LMIC, they are not the only approach available, countries can explore contextually relevant policy experimentation and various alternatives such as test-and-learn approaches, regulatory innovation labs, public-private partnerships, cross-border cooperation, and flexible regulatory frameworks to address regulatory challenges, promote innovation, and enhance the overall digital ecosystem in developing countries (Appiah-Thompson, 2023). To truly foster innovation and sustainable development (Emas, 2015), LMICs may need to consider alternative approaches that prioritize the development of contextual, inclusive, and comprehensive regulatory frameworks, rather than relying solely on a "copy and paste" approach to sandboxes.

3.1.3. Overemphasis on legal frameworks and principles

While the DPF acknowledges the importance of data as a strategic asset, the DPF adopts a predominantly legalistic framework, focusing heavily on compliance with regulations and interopbaility of legal mechanisms (AU, 2022). While this is essential for protecting data rights, it may lead to an overly cautious approach that stifles innovation and the dynamic use of data that support innovation in the African context. In contrast, a just data value creation (JDVC) approach would prioritize framing data as a factor of production for a more balanced approach based on data practitioner challenges emphasises a comprehensive approach to interopbaility, that encompasses various aspects that are crucial for enhancing data governance, facilitating collaboration, and driving innovation across sectors (González Morales & Orell, 2018). A holistic approach to data interopbaility requires a consistent approach to the system-wide improvement of all dimensions (legal, organisational, technical, and semantic) in order to leverage high quality machine-readable data for economic and social benefits, encourage policy experimentation, and anticipatory governance supported by the development of evidence-based solutions (Ahmed, 2023b; González Morales & Orell, 2018)). The DPF's stringent legal requirements may deter organizations from utilizing data creatively, limiting potential innovative data applications in various sectors.

The DPF emphasises a legal perspective of Fair, Reasonable, and Non-Discriminatory (FRAND) principles (AU, 2022), which are primarily concerned with ensuring that data access and usage rights are fair and equitable and are strongly based on contextual realities of EU data ecosystems (Habich, 2022). The FRAND approach aims to prevent discrimination against any party seeking to use data, particularly in contexts where data is essential for competition and innovation. While FRAND principles help establish a legal framework for data sharing, they may not adequately address the technical and operational challenges associated with data interoperability. A strict legal focus can sometimes lead to bureaucratic hurdles that slow down data exchange and inhibit agile responses to market needs (Witting & Kuipers, 2022).

As a more suitable alternative, particularly in the context of enhancing data usability across various platforms and systems, the Findable, Accessible, Interoperable, and Reusable (FAIR) Data Standards are longstanding guidelines for effective data management the emphasize the need for data to be. These principles focus on the technical and semantic aspects of data management, aiming to enhance the usability of data across different platforms and systems (Wilkinson, et al., 2016). FAIR guidelines offer a comprehensive framework that enhances the usability of data across different platforms by focusing on machine-actionability, quality, openness, and adaptability. FAIR principles are arguably more suitable than FRAND for addressing the complexities of modern data management and promoting effective collaboration in a rapidly evolving digital landscape, while fostering responsible innovation and inclusive socioeconomic growth. FAIR promotes rich metadata and clear descriptions that enhance the quality and usability of data. This focus on quality ensures that datasets are not only accessible but also meaningful and reliable for users (GO FAIR, 2024).

FRAND does not inherently address these aspects of data quality and integrity, unlike FRAND, which primarily addresses licensing terms for patents and standards essential for interoperability, FAIR encompasses a broader range of data management practices that aims to enhance the entire lifecycle of data—from creation and storage to sharing and reuse—making it applicable across various domains beyond just technology (GO FAIR, 2024). While FRAND principles provide a necessary legal foundation for equitable data access, FAIR standards address the technical and operational aspects crucial for interoperability and effective data sharing.

For the DPF to effectively facilitate CBDF, promote digital trade, and support the data economy, it is essential to integrate a nuanced understanding of both FAIR and FRAND guidelines to address the complexities and potential disputes that arise from different interpretations. FRAND principles significantly impact the adoption of FAIR data standards by promoting equitable access, legal clarity, and encouraging interoperability and reusability of data. Stakeholders can better leverage both guidelines to enhance data governance and support digital trade, ensuring that legal frameworks, technical standards, data practitioner's realities work in harmony to create a robust data ecosystem, contextualised to African realities.

3.2. Implementation

3.2.1. Emphasis on national data protection authorities

The DPF emphasizes the need for independent data protection authorities (DPA) to develop co-jurisdictional frameworks and mechanisms for oversight and accountability. It suggests that member states should strengthen their regulatory bodies to ensure compliance with data protection standards (AU, 2022). The success of effective mechanisms relies on the political will and resources available to these authorities. The framework does not specify how member states should collaborate to enhance oversight across borders, potentially leading to gaps in accountability and enforcement of data protection measures as countries have varying data protection laws and standards, which can create inconsistencies in how data is managed across borders (Hlomani & Ncube, 2022). This inconsistency

can undermine trust in data-sharing practices and complicate compliance for businesses operating internationally, presenting new challenges for data protection that many DPAs may not be prepared to address. The fast pace of technological advancement and emerging technologies, such as AI and blockchain, can outstrip the ability of DPAs to develop appropriate regulations and guidelines, leaving gaps in governance for CBDF involving most frontier technologies.

Many existing national DPAs in Africa are inadequate to regulate concerns related to data protection and privacy online, particularly for CBDF and digital trade, due to limitations in jurisdiction, inconsistent regulatory standards, resource constraints, lack of independence, weak enforcement, challenges in ensuring adequate protection, rapid evolution of technologies such as AI, complex compliance burdens, and legal uncertainty, to name a few (Kipkoech, 2023). The limitations of domestic DPAs in regulating CBDF for e-commerce and overall digital trade are significant and multifaceted, DPAs operate within the legal frameworks of their respective countries, which restricts their ability to enforce data protection regulations on data that crosses borders. This jurisdictional limitation means that once data leaves a country, the DPA may have little to no authority to ensure compliance with local data protection standards, leading to potential gaps in oversight and protection for individuals (Kipkoech, 2023).

Relying on national DPAs for managing CBDF and digital trade presents several challenges. The fragmentation of regulations across different countries leads to compliance difficulties for businesses, while inconsistent enforcement and jurisdictional conflicts undermine trust in cross-border data exchanges. Moreover, national DPAs may lack the capacity for international collaboration, face bureaucratic delays, and exhibit varying levels of expertise, particularly in dealing with emerging technologies. Political and economic pressures on DPAs can also result in decisions that prioritize national interests over the facilitation of a comprehensive approach to CBDF. A lack of clarity regarding protection and avenues for redress across borders tends to create regulatory uncertainty, which negatively impacts many different dimensions. For example, divergent data privacy and protection regulations at a regional level could hinder the adoption and spread of emerging technologies, potentially reducing their societal benefits (UNCTAD, 2016).

Furthermore, many DPAs operate in isolation and lack formal mechanisms for international cooperation, resulting in fragmented regulatory approaches and difficulties in addressing data protection and privacy issues that span multiple jurisdictions (Hlomani & Ncube, 2022). Beyond domestic DPAs, several other institutions and mechanisms should be involved in regulating CBDF to ensure a comprehensive and effective governance framework (UNCTAD, 2016).

An alternative approach to managing data protection and CBDF for digital trade, beyond relying solely on national DPAs, could involve the creation of regional or continental data governance frameworks that operate across multiple countries, such as the digital protocols of the AfCFTA. The AfCFTA Secretariat could be the more appropriate supranational institution to harmonise, promote consistency, and reduce regulatory fragmentation for CBDF, e-commerce, and digital trade at a continental level. Additionally, mechanisms like mutual recognition agreements (MRAs), regional data trusts, or even existing comprehensive regional data protection frameworks could be leveraged to streamline CBDF and create a unified legal environment for digital trade (UNCTAD, 2016).

3.2.2. Limitations of the African Union Commission

The DPF was endorsed at the continental level by the AU Executive Council in February 2022. The implementation and domestication of the Framework by individual member states appears to be an ongoing process. The framework also acknowledges the unique contexts of each member state, allowing for flexibility in implementation. While this is beneficial, it may lead to a lack of uniformity in data

governance practices across the continent. The absence of stringent enforcement mechanisms could result in varying levels of compliance, potentially undermining the overall objectives of the framework.

However, one key limitation of the DPF is the AUC's lack of binding authority, as it primarily operates through non-binding resolutions and recommendations, allowing MS to selectively implement or ignore AU policies, leading to inconsistent enforcement (Babalola, 2023). The AU's lack of enforcement power significantly limits its ability to ensure compliance with its policies. This challenge is further compounded by the diverse legal and regulatory environments across African countries, making harmonization on regulation related to CBDF, e-commerce, and digital trade difficult and resulting in fragmentation and uneven data protection levels (Hlomani & Ncube, 2022). Additionally, many AU member states struggle with limited resources and capacity, lacking the financial and technical infrastructure necessary to enforce data protection laws effectively. The success of the DPF also heavily relies on the political will and commitment of national governments, which may vary due to more pressing socio-economic challenges or external geopolitical and economic pressures.

Given that ITAs and investment treaties are increasingly incorporating provisions related to cross-border data flows and digital trade. Negotiating provisions for CBDF through the AfCFTA, can potentially create a more predictable and stable environment for e-commerce and digital trade, such as the AfCFTA Secretariat's Digital Trade Protocols.

Furthermore, multistakeholder initiatives involving governments, the private sector, civil society, academia, and technical communities are crucial to contributing to the development of norms, standards, and best practices for CBDF, e-commerce, and digital trade. Consolidating the knowledge and resources from various initiatives can foster policy coherence and coordination, promote transparency, and ensure that diverse perspectives are considered in the policymaking process. Effective collaboration amongst stakeholders can facilitate cooperation, promote best practices, and develop dispute-resolution mechanisms to address conflicts arising from data governance issues.

A multi-layered approach involving various institutions and mechanisms is necessary to address the complexities of CBDF. By combining the efforts of domestic authorities, regional bodies, international organizations, trade agreements, multistakeholder initiatives, industry self-regulation, judicial mechanisms, and capacity-building programs, countries can create a more coherent and effective data governance landscape that supports digital trade and innovation while protecting individual rights.

3.3. Scope

3.3.1. Data interoperability and data governance

Data interoperability, cross-border data flows, and data governance are interdependent elements that collectively shape the landscape of global data exchange for effective digital trade (FSB, 2023). Understanding their relationship is essential for fostering a secure and efficient data exchange environment. In the context of data flows, data interopbaility involves the compatibility of data formats, protocols, and regulations across borders. As mentioned earlier, effective (legal and non-legal)[3] interoperability mechanisms are essential for enabling smooth cross-border data exchanges through agreements on data privacy principles and the development of common data classification systems, which facilitate trust and collaboration among countries (Bank, 2022). By establishing common standards and protocols, interoperability allows for the seamless exchange of data across borders, reducing barriers caused by differing regulations. In a highly networked world, legal interoperability is a

[3] Legal interoperability focuses on aligning legal frameworks, policies, and regulations to ensure organizations operating under different jurisdictions can work together. Non-legal interoperability emphasizes technical, semantic, organizational, and cultural aspects to facilitate data sharing without relying solely on legal mechanisms.

complex issue. The negative impacts of non-interoperable laws can create regulatory arbitrage. On the other hand, other (non-legal) dimensions of data interoperability are also as important to create public value from data such as technical integration, semantic alignment, and organizational change management (González Morales & Orell, 2018).

The DPF emphasizes the need for harmonized national data systems, which is crucial for achieving interoperability among African nations. It advocates for the integration of disparate data systems into cohesive structures that facilitate access and sharing across borders, from a legal approach. However, the implementation of these recommendations may face challenges due to the varying levels of digital maturity and regulatory environments among member states. The DPF does not provide specific, actionable guidelines to ensure that countries can effectively harmonize their data ecosystems, which could lead to inconsistencies in how the different dimensions of interoperability is achieved across the continent. Furthermore, effective data governance is crucial for non-legal aspects of interoperability, which involves establishing trustworthy data management practices, ensuring data quality and security, and promoting data stewardship across government entities (Bank, 2022). A well-designed data governance framework can facilitate data sharing while maintaining appropriate controls and safeguards. By focusing on non-legal aspects of interoperability governments can create an enabling environment for data exchange and collaboration without relying solely on legal mechanisms. This approach can lead to more efficient and effective public service delivery, better-informed decision-making, and improved outcomes for citizens.

Furthermore, the DPF emphasizes the need for MS to create a legal environment that fosters data flows while ensuring adequate protection for personal data. It calls for the establishment of national laws that align with regional standards, promoting a harmonized legal ecosystem.

However, the effectiveness of these legal mechanisms depends on the willingness and capacity of individual countries to implement them. Many MS have historically been slow to adopt progressive data protection laws, which could hinder the framework's objectives of interoperability and seamless data exchange across borders. While there are many definitions, robust data governance encompasses the policies, regulations, and practices that dictate how data is managed and protected (Aaronson, 2021). Robust data governance is central to ensuring that CBDF occur in a secure and trustworthy manner.

3.3.2. Gender inequality and digital trade

Women often encounter significant financial challenges when trying to engage in digital trade (Sirimanne & Adhikari, 2023). While the DPF broadly emphasises, a human rights-based approach, it does not explicitly mention or incorporate gender-specific considerations in its guiding principles, data governance strategies, or implementation plans. Consequently, the DPF has limitations to recognize the unique challenges and barriers women face in accessing and participating in the data economy, such as the digital gender divide and gender-based violence online. The DPF also lacks specific provisions for ensuring that gender equality and women's empowerment are prioritized in the development of data ecosystems and the utilization of data for economic growth. Without a gender mainstreaming approach, the framework risks perpetuating existing gender disparities in the digital sphere (Ahmed et al., 2021).

Furthermore, the DPF does not reference or align with the African Union Strategy for Gender Equality and Women's Empowerment, which provides a comprehensive framework for promoting gender equality and women's empowerment across various sectors (AU,2019). Mainly due to the narrow legal scope, the DPF does not emphasize the importance of collecting and utilizing gender-disaggregated data to monitor and evaluate the impact of data policies on women and men. Without such data, it becomes challenging to assess the progress made in addressing gender inequalities and ensuring equitable participation in e-commerce, digital trade, and the overall data economy.

Women-led businesses often face gendered supply-side and demand-side constraints that affect their ability to engage in cross-border trade (IFC, 2024), which include difficulties in accessing information about compliance requirements, limited technical capacity, and a higher share of unpaid work. Women entrepreneurs, particularly those running micro, MSMEs often face increased regulatory burdens. The complexity of compliance with non-tariff measures (NTMs) can disproportionately affect women-led businesses, as they may lack the resources to navigate these regulations effectively. This can lead to higher costs and reduced capacity to engage in cross-border trade (IFC, 2024; UNCTAD, 2023).

3.3.3. Data governance and environmental sustainability

Climate change is a global issue that requires comprehensive data collection from different geographical areas to understand regional variations and global patterns. By allowing scientists and researchers to access data from multiple sources, cross-border data flows can enhance the robustness and reliability of climate models (Randall et al., 2018). The DPF has notable shortcomings in addressing climate change and environmental data considerations. The DPF does not explicitly address the environmental implications of data management practices. As data generation and usage increase, so does the environmental impact associated with data centres, energy consumption, and electronic waste (UNCTAD, 2024). By failing to incorporate guidelines or recommendations for sustainable data practices, the framework overlooks the urgent need to align data governance with environmental sustainability.

Furthermore, the DPF does not recognize the critical role that robust data governance can play in climate monitoring, reporting, and analysis (Sebestyén et al., 2021). Climate data is essential for understanding and mitigating the impacts of climate change, yet the DPF lacks provisions for the collection, sharing, and utilization of environmental data. This omission limits the potential for data to be leveraged in addressing climate-related challenges and supporting sustainable development initiatives.

The DPF operates in isolation from existing environmental policies and initiatives within the AU. By not integrating data governance with broader environmental strategies, the framework misses' opportunities to create synergies that could enhance both data management and environmental sustainability. A more holistic approach would ensure that data governance supports the AU's environmental goals. Several regions have successfully integrated environmental considerations into their data policies, showcasing effective strategies for balancing data governance with sustainability. The European Union (EU) has been a leader in this area, incorporating environmental policy integration (EPI) into its directives, such as the General Data Protection Regulation (GDPR) and the European Green Deal (Finck & Mueller, 2023). There are also calls to create databases to measure the environmental impact of data-based systems such as AI (OECD, 2022).Initiatives that emphasize the importance of data governance to support sustainability in data management and data sharing for environmental protection across borders require access to comprehensive data, which allows stakeholders to assess the impacts of climate change, evaluate mitigation strategies, and implement adaptation measures (Randall et al., 2018).

Robust data governance can enhance global climate modelling efforts by providing access to diverse data sources, fostering collaboration among researchers, improving climate predictions, enhancing disaster response efforts, supporting the development of renewable energy technologies, and informing policy development to support more coordinated and effective response to climate change, ultimately contributing to global sustainability efforts and the achievement of climate-related goals (Sebestyén et al., 2021).

4. Case Study Analysis: South African Customs Union (SACU)

4.1. Significance of the South African Customs Union (SACU)

The DPF encourages regional collaborations as pivotal frameworks for fostering collective efforts among neighbouring nations to address common data governance challenges and pursue shared objectives (AU, 2022). As the continent embraces robust data governance to support digital transformation, it is crucial to assess the suitability of the DPF to foster digital trade and the movement of data within existing trade blocs such as SACU comprising Botswana, Lesotho, Namibia, Eswatini (BLNS) and South Africa (SACU, 2024).

Customs unions are interesting to study for continental digital trade integration and CBDF as they can provide insight into an existing framework for economic collaboration, regulatory harmonisation, and create opportunities for enhancing trade efficiency and competitiveness in the data economy (Abrahams et al., 2023). SACU members agree on a common external tariff (CET) and trade policies towards non-members. The CET can be an existing tool to create a consistent regulatory environment for CBDF, as MS can make use of the CET to align their positions on data protection, privacy, and digital trade provisions in external agreements.

SACU already has a mechanism for collecting and distributing physical trade tariff revenues among members, which can serve as a foundation for broader data governance frameworks and digital dividends (Zieliński, 2017). The common negotiating mechanism, established under Article 31 of the SACU Agreement, allows member states to negotiate trade agreements with third parties as a bloc. This unified approach ensures that the interests of all member states are represented, promoting a cohesive strategy for engaging in international trade, including digital trade and data flows. This harmonization can facilitate the development of common data governance frameworks and standards that support CBDF and digital trade within the union. The existing efforts to reduce the administrative and financial burdens associated with cross-border transactions can encourage businesses to engage in digital trade and share data more freely across borders (Abrahams et al.,2023.).

The larger, more integrated market that a customs union provides can enable businesses to achieve economies of scale and increase their competitiveness, which can drive innovation and investment in digital technologies and data-driven solutions that support cross-border trade.

A matter of interest is that the revenue-sharing formula relies on accurate data from MS on imports, exports, GDP, and other economic indicators. Improving data management systems, data sharing, and efforts in measuring the data economy between SACU countries could help optimize the formula's implementation and enable better monitoring of digital trade flows (UNCTAD, 2023). The formula creates incentives for SACU MS trade policies based on their potential impact on customs and excise revenues due to changes in tariffs and trade patterns, which could influence how countries approach digital trade regulations and CBDF policies.

The formula's distribution of revenues is often seen as inequitable, with some MS benefiting more than others (Cuevas, 2013). Unresolved equity issues could spill over into discussions on digital trade policies and regulations within SACU. The establishment of a customs union often goes hand in hand with increased political cooperation and integration among member states, which creates an environment conducive to developing shared policies and regulations related to data governance, privacy, and digital trade (Abrahams et al., 2023).

However, it's important to note that the effectiveness of a customs union in supporting data governance, cross-border data flows, and digital trade depends on several factors, including the specific provisions

of the union, the level of political commitment, the capacity of member states to implement and enforce common policies and standards, and the evolving nature of digital trade regulations globally (Abrahams et al., 2023).

Furthermore, one of the primary challenges for SACU is the need for regulatory harmonization amongst member states. Currently, SACU countries have varying regulations regarding data protection, e-commerce, and digital-enabled services, which can create barriers to seamless digital trade. This variation includes the need for trade-related considerations such as advanced customs systems, digital payment solutions, and reliable internet connectivity, amongst others. Without sufficient infrastructure, the integration of digital trade, including leveraging CBDF, may be limited.

A matter of concern is that while data is crucial for e-commerce and digital trade, existing multidimensional structural inequality within SACU means that datafication of economic activity will have uneven implications for different groups and communities, with potentially devastating intergenerational effects that worsen existing economic mobility and inequality of opportunity in a data-driven economy (Ahmed, 2023a; Sulla et al., 2023). SACU represent the world's most unequal region though there are differences across countries with Namibia and South Africa distinctly having higher inequality than the rest and Lesotho the least (Sulla et al., 2022). A techno-optimist approach to digitalisation may risk further entrenching inequality or creating new forms of marginalisation (Ahmed et al., 2023).

Lastly, existing customs agreements with third parties may not adequately address the complexities of digital trade, raising the need to modernize these agreements to incorporate provisions for digital goods, services, and data flows, which can be a politically sensitive issue among member states (Hlomani & Ncube, 2022).

4.2. SACU's adoption of AU Frameworks

As a complementary document to existing initiatives the DPF endorsed in February 2022, provides a comprehensive roadmap for African countries to harness the power of data for sustainable development, evidence-based decision-making, and addressing continental challenges (AU,2022).

The Draft AfCFTA Digital Protocol establishes an important legal instrument that will, through harmonized rules and common principles and standards, support and enable an acceleration of technology-driven innovation and commerce in Africa. It focuses on promoting intra-African digital trade, enhancing cooperation on digital matters among signatories of the AFCFTA, and creating a transparent, secure, and trusted digital trade ecosystem. SACU considers the AfCFTA a vital continental instrument. All SACU MS have ratified the AfCFTA Agreement, and as such, its implementation and strategic utilization have been prioritized as a key pillar in the SACU Strategic Plan for 2022–2027 (SACU, 2024).

In 2014, the African Union (AU) Convention on Cyber Security and Personal Data Protection adopted a legal framework for addressing cybercrime and data protection in Africa. To date only fifteen AU MS have adopted the Malabo Convention, including Namibia, the only SACU MS that has adopted the Malabo Convention.

4.3. SACU Assessment for Digital Trade

The SACU assessment consists of secondary data analysis that are highly related to digital trade, such as CBDF and e-commerce and for which there is wide country coverage amongst SACU MS such as data on account ownership at a financial institution or with a mobile-money-service provider, Percentage of

individuals using the Internet, the integrated index for postal development (2IPD), secure Internet servers and the digital adoption index (DAI).

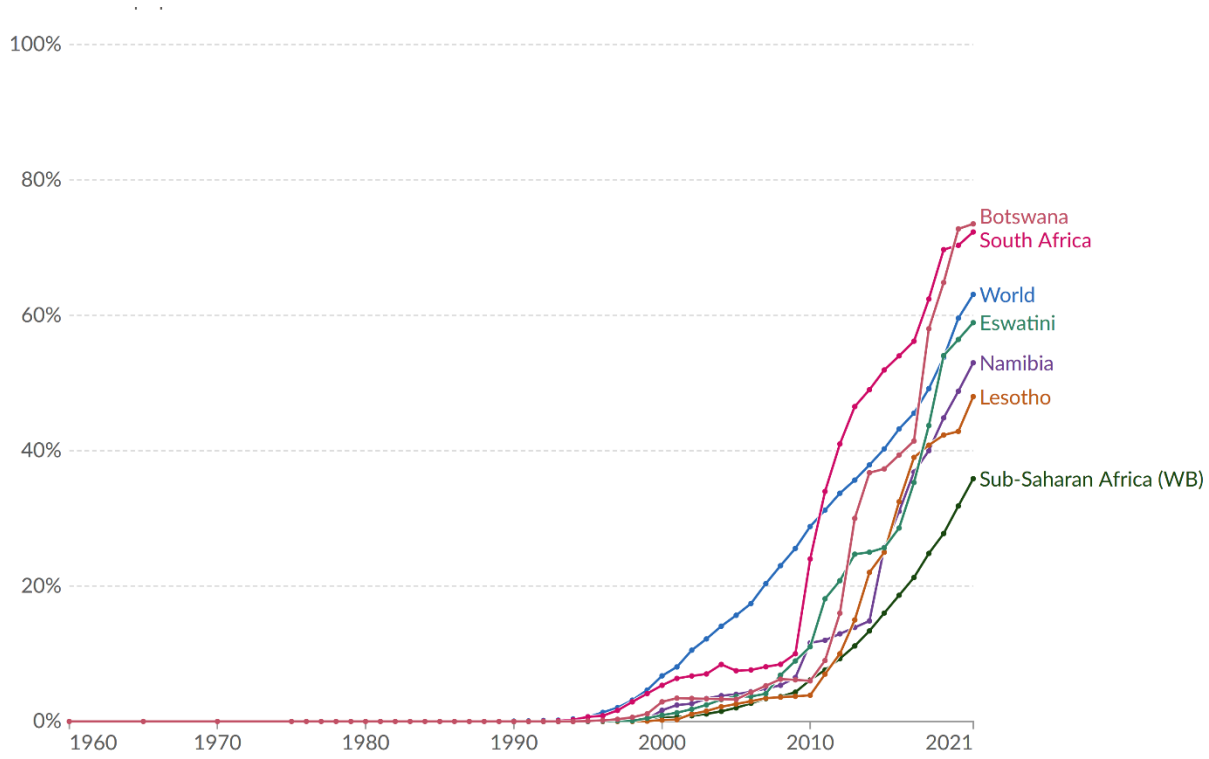
In addition, the assessment includes a high-level summary of the SACU policy and regulatory environment for digital trade, CBDF, and e-commerce and data economy enablers of SACU MS.

4.3.1. Importance of Internet usage for digital trade

Understanding the share of the population using the Internet among SACU countries —Botswana, Namibia, Eswatini, Lesotho, and South Africa are critical for realizing the benefits of a DSM. Internet access influences market potential, facilitates CBDF, e-commerce, enhances digital literacy, informs infrastructure investment, and boosts regional competitiveness (World Bank, 2016).

Meaningful connectivity is linked to economic development, countries with a larger share of the population online can leverage digital technologies to drive innovation, improve productivity, and create jobs (World Bank, 2016).

Figure 1: Share of the population using the Internet



Source: International Telecommunication Union

Figure 1, highlights that while SACU countries generally have internet usage rates above the SSA average of approximately 36 percent, there is variation amongst MS due to various factors such as infrastructure challenges, ineffective institutions, and economic constraints, to name a few.

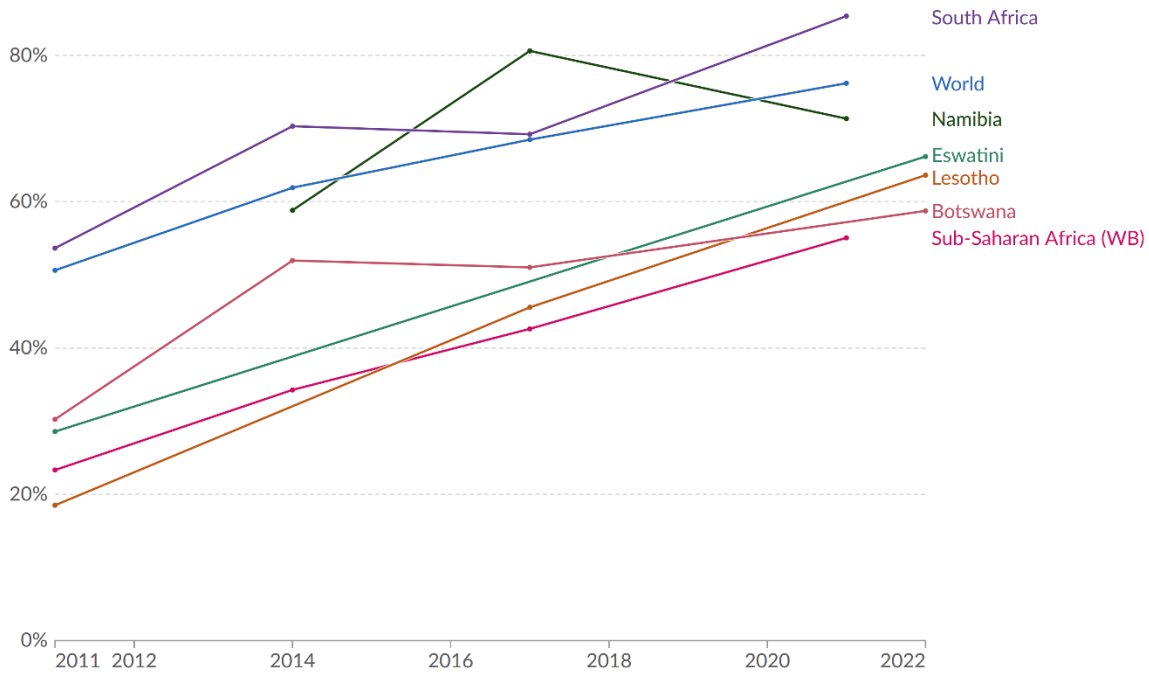
Botswana and South Africa lead the region in digital connectivity with over 70 percent of the population in the respective countries using the Internet, higher than the world average of 63 percent. A higher percentage of internet users in SACU countries indicates greater potential for businesses to engage in digital trade. Increased internet penetration allows more individuals and businesses to access online marketplaces, facilitating participation in e-commerce. This is particularly important for MSMEs that may rely on online platforms to reach customers beyond their local markets, which could potentially

contribute to overall economic resilience and competitiveness in the global market. The share of the population using the Internet also reflects the effectiveness of infrastructure investments and policy initiatives aimed at enhancing connectivity (World Bank, 2016).

4.3.2. Access to a formal financial institution

Access to formal financial institutions is crucial for fostering a vibrant digital trade environment among SACU countries. robust network of formal financial institutions can facilitate the harmonization of financial regulations across SACU countries. Alignment is crucial for creating trustworthy and secure seamless payment systems that facilitate the DSM. Mobile banking and digital payment solutions offered by formal institutions can reach remote areas where traditional banking services are limited, thus expanding the customer base for e-commerce, particularly or women (IFC,2024) Access to banking services enables consumers and businesses to conduct online transactions confidently, fostering a robust digital marketplace.

Figure 2: Share of adults with an account at a financial institution[4]



Source: World Bank

Figure 2 reveals that approximately 85 percent of adults in South Africa have an account at a financial institution., higher than both the World average of 76 percent and SSA average of 55 percent. While South Africa leads in financial inclusion within SACU, there are clear disparities amongst MS —71 percent of adults in Namibia have an account at a financial institution, 66 percent of adults in Eswatini and 64 percent of adults in Lesotho have an account at a financial institution, there is still significant room for improvement in Botswana, where approximately less than 58 percent of adults have an account at a financial institution . Addressing these disparities is essential for realizing the full benefits of digital trade and regional integration.

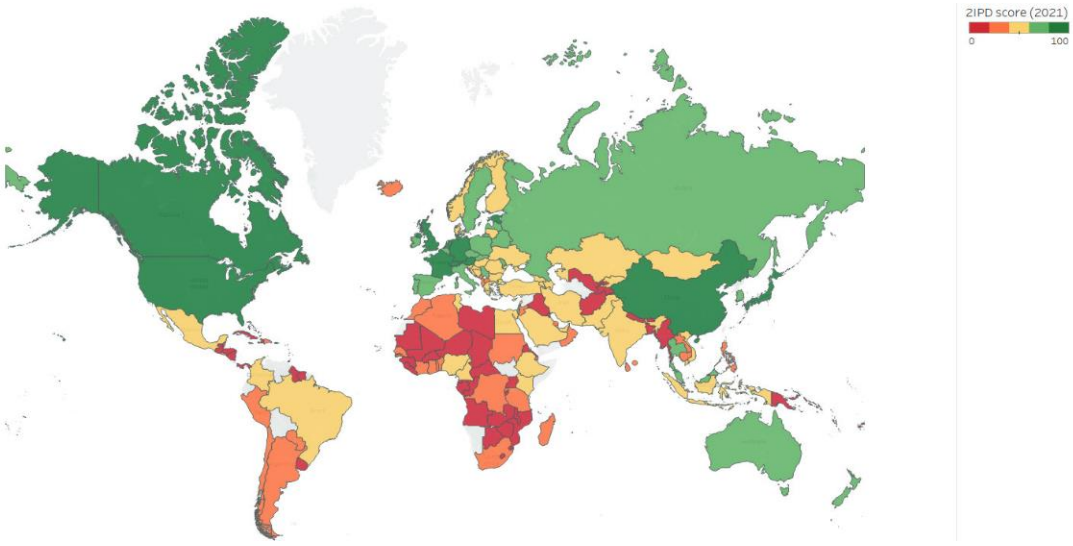
[4] The share of respondents aged 15 and older, who report having an account (by themselves or with someone else) at a bank or another type of financial institution.

4.3.3. Integrated Index for Postal Development (2IPD)

The Integrated Index for Postal Development (2IPD)[5] provides a comprehensive view of global postal development that is essential for understanding and enhancing e-commerce, reflecting ease of receiving parcel deliveries from online transactions (UNCTAD, 2018; UPU, 2022). The 2IPD provides a detailed evaluation of postal services across 172 countries, measuring factors such as reliability, reach, relevance, and resilience. This comprehensive view allows stakeholders to understand the current state of postal infrastructure globally, which is crucial for facilitating digital trade. Reliable postal services are essential for the timely delivery of goods purchased online, making them a backbone of e-commerce (UNCTAD,2018).

Figure 3 below highlights that there are significant geographical disparities in postal development across the world. As a region, SSA has median 2IPD score of 16.3, well below the global median 2IPD score of 30.0, which —the larger the postal development inequalities between countries and regions, the more complex it becomes to optimally design future international postal exchange platforms for the data economy that can integrate stakeholders to benefit from postal services (UPU, 2022).

Figure 3: Global 2IPD score distribution



Source: Universal Postal Union

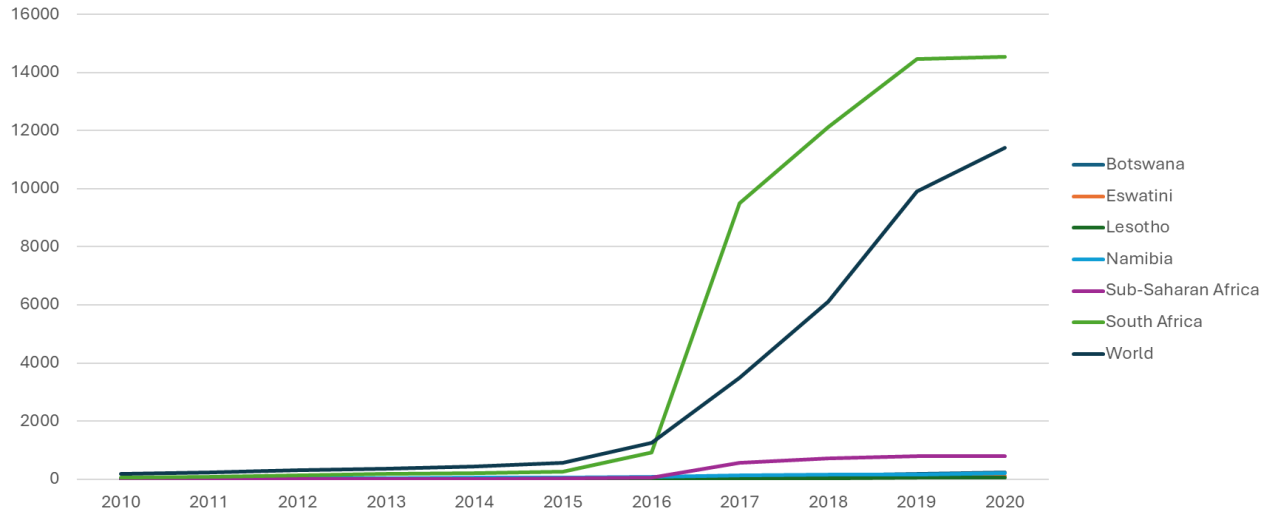
4.3.4. Secure Internet servers

Analysing the number and quality of secure internet servers[6] is crucial for understanding the digital trade landscape, CBDF, and e-commerce potential in the SACU countries, secure servers directly impact the trust, efficiency, and scalability of digital transactions, particularly as a proxy for e-commerce (UNCTAD, 2018). Secure internet servers, which support encrypted transactions, are fundamental for ensuring the safety of digital trade and e-commerce activities. Businesses and consumers need to trust that their

[5] The 2IPD scoring system is built around the four key dimensions of postal development: postal reliability, reach, relevance and resilience, also referred to as the "4Rs" of postal development.
[6] The number of distinct, publicly trusted TLS/SSL certificates found in the Netcraft Secure Server Survey.

data—such as financial information—is secure from breaches or cyberattacks when conducting cross-border online transactions (UNCTAD, 2018).

Figure 4: Secure Internet servers amongst SACU (per 1 million people)



Source: World Bank

Figure 4[7] showcases that in 2020, South Africa had the highest availability of secure servers, more than 14 000, per 1 million people, above both the SSA and World average approximates of 788 and 11 000 (per 1 million people) respectively. A matter of concern is that in the same year, the other SACU MS, have dismal numbers of secure Internet servers per 1 million people (see Annex A for further details).

SACU needs robust, secure server infrastructure to attract investments, facilitate CBDF, digital trade, and boost their participation in global e-commerce (UNCTAD, 2018). Digital trade relies heavily on the seamless and secure exchange of data across borders. Secure servers ensure that the data flows between SACU countries and international partners are safe from unauthorized access, protecting sensitive business information and personal data. Without adequate secure server infrastructure, cross-border data flows could be hindered, leading to mistrust and a reluctance from businesses to engage in international digital commerce (UNCTAD, 2019).

4.3.5. Digital adoption amongst SACU Member States

The DAI provides a comprehensive measure of digital adoption benchmarked across three dimensions: people, government, and business. This benchmarking allows SACU countries to assess their digital readiness relative to one another and to other countries globally. By identifying strengths and weaknesses in digital adoption, policymakers can develop targeted strategies to improve their digital ecosystems (World Bank, 2016).

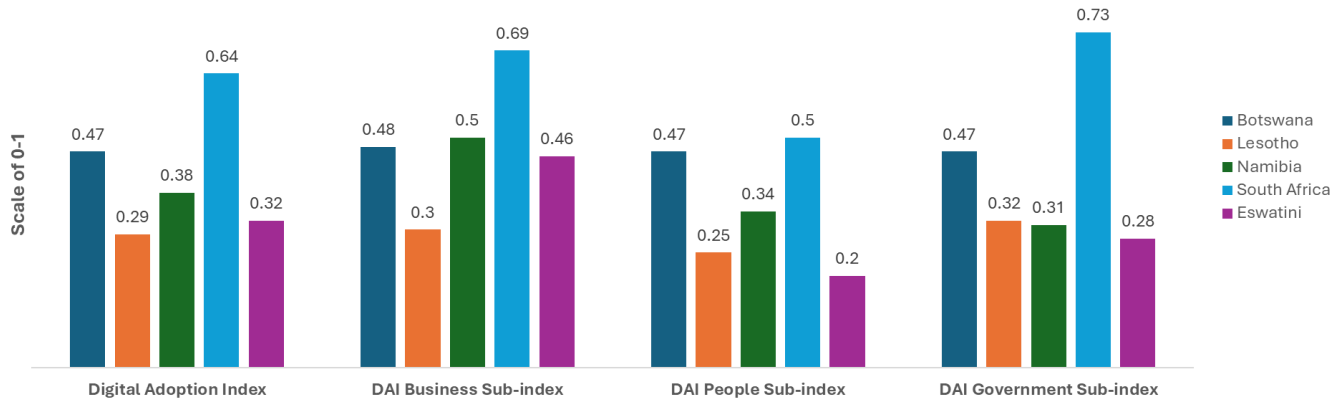
According to the digital adoption index (DAI)[8] , Figure 5 highlights the uneven digital adoption amongst SACU MS, across all three dimensions of the economy: people, government, and business. Each sub-index comprises technologies necessary for the respective agent to promote development in the digital

[7] See Appendix A

[8] The Digital Adoption Index (DAI) is a composite index measuring the extent of spread of digital technologies within and across countries worldwide. The index covers 180 countries on a 0–1 scale and emphasizes the "supply-side" of digital adoption to maximize coverage and simplify theoretical linkages. The DAI can assist policymakers in designing a digital strategy with tailored policies to promote digital adoption across different user groups.

era: increasing productivity and accelerating broad-based growth for business, expanding opportunities and improving welfare for people, and increasing the efficiency and accountability of service delivery for government.

Figure 5: Digital Adoption between SACU Member States [9]



Source: World Bank

South Africa has scores closer to 1 which reflects the extent to which digital technologies are available and adopted by all the key agents in the South African economy (people, businesses (firms), and governments) (World Bank, 2016).

Figure 5 also reveals that in SACU countries, while business adoption is increasingly high, people gaining access to digital technologies remains surprisingly lower, particularly in Eswatini (Swaziland). The disparity between business adoption an adoption by the public calls for policymakers to explore barriers to uptake, which may extend beyond the information and communication technologies (ICTs) sector, such as high price of mobile devices, Internet access costs, or quality and availability of existing networks (World Bank, 2016).

[9] Based on 2016 data

4.3.6. SACU Policy and Regulatory Assessment for Digital Trade

Table 1: High-level SACU Policy and Regulatory Assessment for Digital Trade

	Indicator						
Country	**Data Governance Policies**	**E-commerce Policies**	**Participation in trade agreements committing to open cross-border data flows**	**Data privacy and protection regime**	**Local storage requirement**	**Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement)**	**Information Technology Agreement (ITA)**
Botswana	Data Protection Act (2018)	E-Commerce Strategy (2015)	Botswana has not joined any free trade agreement committing to open transfers of cross-border data flows	**Conditional Flow Regime.** Transfer of data is not prohibited in Botswana but there are exceptions on personal data.	No local data storage requirements	As a member of the WTO, Botswana is a party to the TRIPS Agreement since 1995.	Not signatory to ITA
Eswatini	Electronic Communications and Transactions Act (2007) Data Protection Act (passed in March 2022)	E-Government Master Plan (2013)	Eswatini has not joined any free trade agreement committing to open transfers of cross-border data flows.	**Conditional Flow Regime.** Transfer of data is not prohibited in Eswatini, Section 33(3) of the Act lists conditions	No local data storage requirements	As a member of the WTO, Eswatini is a party to the TRIPS Agreement since 1995.	Not signatory to ITA
Lesotho	Data Protection Act (Act No. 5 of 2012, adopted on 22nd February 2012) Communications Act (Act No. 4 of 2012 adopted on 17th February 2012)	E-Government Strategy (2014)	Lesotho has not joined any free trade agreement committing to open transfers of cross-border data flows	**Conditional Flow Regime.** Transfer of data is not prohibited in Lesotho but there are exceptional cases (Section 29 of the Act).	No local data storage requirements	As a member of the WTO, Lesotho is a party to the TRIPS Agreement since 1995.	Not signatory to ITA
Namibia	Communications Act (2009)	E-Governance Policy (2005)	Namibia has not joined any free trade agreement committing to open transfers of cross-border data flows.	No regulations governing cross-border data flows on Namibia,	No local data storage requirements	As a member of the WTO, Namibia is a party to the TRIPS Agreement since 1995.	Not signatory to ITA
South Africa	Protection of Personal Information Act (POPIA, 2013)	National E-Commerce Policy Framework (2019)	South Africa has not joined any free trade agreement committing to open transfers of cross-border data flows.	**Conditional Flow Regime.** Transfer of data is not prohibited in South Africa but there are exceptions on personal data.	No local data storage requirements	As a member of the WTO, South Africa is a party to the TRIPS Agreement since 1995.	Not signatory to ITA

Source: National Government Websites and Ferracane et al, 2023

Table 1 evaluates the digital trade landscape amongst SACU MS focusing on key areas such as data governance policies, e-commerce policies, and participation in trade agreements that commit to open cross-border data flows, to name a few. All SACU MS are signatories to the African Continental

Free Trade Agreement (AfCFTA), which includes provisions for promoting open cross-border data flows, a crucial step for facilitating digital trade across the region. All SACU MS are bound by the TRIPS Agreement, which sets minimum standards for intellectual property protection. However, varying levels of enforcement and understanding of these standards exist among member countries.

While SACU member states have made progress in developing data governance and e-commerce policies, there are still gaps and inconsistencies across the region that will impact efforts to create a regional DSM, let alone the continental DSM. Significant disparities exist among member states regarding implementation capacity and regulatory frameworks.

SACU states and many African countries are not signatories to the WTO Information Technology Agreement (ITA) for several reasons, reflecting broader concerns about global digital trade, economic sovereignty, and revenue generation. South Africa, along with other developing countries like India and Indonesia, position on the e-commerce moratorium further illustrates the discontentment with the multilateral trading system (MTS), there are concerns that the (MTS) disproportionately benefits wealthier nations with established tech industries at the expense of LMICs struggling to build their own data economies (UNCTAD, 2020).

Understanding the regulatory landscape of digital trade within SACU helps identify barriers and opportunities for integration among MS. A coordinated approach to governance can facilitate smoother cross-border transactions, further promote intra-regional digital trade, and align with broader initiatives like the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol.

Table 2: High-level analysis of Data Economy Enablers of SACU Member States

	Country				
Enablers	**South Africa**	**Botswana**	**Lesotho**	**Namibia**	**Eswatini**
Data Governance	Progress in establishing data governance structures at existing institutions. Currently multiple siloed approaches, further development needed for comprehensive guidelines and frameworks.	Limited data governance frameworks, need for clear guidelines and institutions.	Lacks well-defined data governance structures and policies. Significant development needed.	Some steps taken towards data governance. Lacks comprehensive framework for accountability and transparency.	No clear data governance structure. Need to prioritize guidelines and institutions for effective governance.
Data Infrastructure	Relatively well-developed critical data infrastructure, including, data centers and digital platforms; challenges in resilience and efficiency with stable electricity access.	Limited data infrastructure. Need investment in data centres, networks, and digital platforms.	Underdeveloped data infrastructure; requires significant investment.	Limited data infrastructure. Prioritization of data centers and platforms needed.	Underdeveloped data infrastructure. Basic infrastructure required.
Data Privacy and Protection	Progress with the Protection of Personal Information Act (POPIA). Further alignment with international standards needed.	Limited measures. Needs more comprehensive legislation and regulations for data protection.	Lacks frameworks. Needs significant efforts to develop legislation and align with international standards.	Some steps taken. Lacks comprehensive data protection framework.	Progress with Data Protection Act passed in March 2022.
Data Accessibility and Openness	Progress in promoting accessibility and openness through initiatives like the Open Government Partnership. Further efforts needed to encourage data release and innovation.	Limited initiatives. Need to promote data accessibility and facilitate research.	Lacks initiatives. Requires development to encourage data release and innovation.	Some steps towards accessibility and openness. Lacks comprehensive approach.	No initiatives. Needs to prioritize data release and innovation.
Capacity Building	Progress in capacity building, e.g., Digital Skills for the Future. More efforts needed to enhance data literacy and digital capabilities	Limited initiatives. Need prioritization of data literacy and digital capabilities.	Lacks initiatives. Requires development and implementation of capacity-building programs.	Some steps towards capacity building. Lacks comprehensive approach to enhance data literacy and digital capabilities.	No initiatives. Needs prioritization of data literacy and digital capabilities.

Source: Authors own analysis from various sources

The data economy enablers—data governance, infrastructure, privacy protection, accessibility, and capacity building—are interconnected elements that play a critical role in facilitating cross-border data flows (CBDF), digital trade, and e-commerce. Together, these components are crucial for SACU member states to effectively navigate the data economy and enhance their competitiveness in regional and global markets. By strengthening their endowments, capabilities, and enablers, SACU countries can better leverage digital trade opportunities, improve economic integration, and address challenges such as the digital divide and regulatory inconsistencies. Table 1 reveals that SACU's member states have varying levels of digital

infrastructure and economic development, representing a microcosm of the challenges and opportunities in African regional integration through digital trade (WTO, 024). South Africa leads in establishing data governance structures, infrastructure, data privacy and protection, accessibility, and capacity-building initiatives. However, other SACU members, particularly Lesotho and Eswatini, require substantial efforts to develop and align their frameworks and initiatives with the AU DPF. Addressing these gaps is crucial for realizing the full benefits of a data-driven economy and regional integration under the AfCFTA.

5. Key Findings

Efficient intra-regional trade and supply chain management relies on the smooth flow of goods, services, capital, and data — thus cross- border movement of data is essential to many aspects of e-commerce and digital trade. But digital trade and e-commerce do not exist in isolation, they require several complex cross-cutting considerations for regulatory convergence, harmonisation of legal frameworks, internet governance, information and communications technologies (ICTs) policy reform, and strategic regional ICTs infrastructure investments and implementation, to name a few.

The SACU case study provides a detailed examination of how the Data Policy Framework (DPF) can be applied to support continental integration objectives, particularly within the context of digital trade. SACU's approach to trade facilitation can inform the DPF's emphasis on policy coherence and public sector innovation. Systems thinking and anticipatory governance should be employed to ensure that digital trade policies are aligned and mutually reinforcing, addressing the complex interdependencies within the data economy. While SACU countries generally have better internet penetration than some of their Sub-Saharan counterparts, gaps in secure internet infrastructure still exist. A transversal approach and understanding of the interconnection amongst cross-cutting issues is crucial to mitigate risks and address both barriers and opportunities in creating a rights-respecting digital single market (DSM) powered by data. Only by thinking and working beyond silos, designing holistic digital strategies for sustainable impact, and applying a people-centred approach to their policies and investments will international development actors be able to deliver on the mission of an inclusive and just digital future.

To fully harness the benefits of the digital revolution, countries must also focus on "analog complements"—strengthening regulations that promote business competition, equipping workers with skills suited to the evolving economy, and ensuring that institutions remain transparent and accountable.

Disparities in digital infrastructure and internet access among SACU member states (MS)—South Africa, Botswana, Namibia, Eswatini, and Lesotho—can hinder digital trade, regional integration, cross-border data flows (CBDF), and e-commerce. SACU Countries with weaker digital maturity may struggle to participate in regional digital markets, creating imbalances in competition and limiting seamless data exchanges. These gaps also restrict e-commerce growth and prevent less-connected nations from fully integrating into a regional data economy, ultimately weakening overall economic cohesion and opportunities for inclusive development within SACU.

In general, along with supply side indicators, other demand-side indicators—such as workforce skills, business sector competition, and government accountability are crucial elements to identify the right mix of digital and "analog" policies needed to accelerate digital transformation within SACU MS. Overall, all SACU MS need a coherent collaborative approach to supply-side policies that support availability, accessibility, and affordability , while simultaneously fostering demand side policies that focus on making the internet universal, affordable, open , and safe particularly with new waves of frontier technologies such as artificial intelligence (AI).

Getting the foundations right is essential for a trusted, sustainable, and inclusive digital future, and requires policy attention to respond to crucial challenges. **See Appendix B.**

6. Conclusion

The African Union's Data Policy Framework (DPF), while designed to ensure data sovereignty and address continent concerns, is not fully appropriate for fostering a Digital Single Market, cross-border data flows (CBDF), digital trade, and e-commerce across the Southern African Customs Union (SACU) member states (South Africa, Botswana, Namibia, Eswatini, and Lesotho) and Africa in general. This is because the DPF's emphasis on national data protection authorities as institutions to lead data governance can lead to fragmented regulations that conflict with the transnational nature of digital technologies and data, which inherently transcend borders. For digital trade and CBDF to thrive, countries need interoperable laws and policies along with other factors that facilitate seamless data exchanges and technology adoption across borders. The DPF's focus on legal dimensions without adequate regional collaboration on other factors that are crucial for trustworthy regional data ecosystems risks creating barriers to trade, increasing regulatory complexity, and limiting market integration, which can stifle the growth of e-commerce and digital trade. A proactive sociotechnical approach is essential to address the complex interplay within the data economy, particularly if digital technologies are used for the public good. A proactive stance allows for timely interventions that can mitigate risks and enhance the effectiveness of public policies

Developing a harmonized approach to data governance across Africa through the Digital Protocols of the Africa Continental Free Trade Area (AfCFTA) could be a more appropriate approach to facilitate CBDF and support the growth of digital trade on the continent as opposed to the DPF.

7. Recommendations

Based on the key findings regarding the importance of CBDF for e-commerce and digital trade in Africa, the following recommendations are tailored for specific categories of stakeholders**:**

Governments/Public sector

Develop comprehensive public sector innovation policies that support robust data governance: To foster public sector innovation (PSI), it is essential to create an environment that encourages creativity and experimentation. Governments should prioritize the creation of robust data governance frameworks that align with international best practices while considering local contexts. This could include establishing clear regulations on data protection, privacy, building human capital, and ownership to facilitate secure cross-border data flows.

PSI can be achieved through leveraging existing expertise or building capacity of public servants by leveraging local expertise to support the establishment of dedicated innovation hubs within government agencies that focus on developing new ideas and solutions tailored to address specific public needs. Training programs should focus on equipping public servants with the skills necessary to embrace innovative practices, including design thinking, data analytics, and collaborative problem-solving. These hubs can serve as platforms for collaboration among various stakeholders, including civil society, academia, and the private sector, fostering a culture of co-creation.

Build public sector capacity for anticipatory governance and decolonial sociotechnical foresight: Capacity building is crucial for fostering a culture of innovation within the public sector. Training programs should focus on equipping public servants with the skills necessary to embrace innovative practices, including design thinking, data analytics, and collaborative problem-solving. By implementing these strategies, public sector innovation can thrive, enabling governments to respond effectively to current challenges while anticipating future needs. This holistic approach will

not only enhance service delivery but also strengthen democratic governance by actively engaging citizens in shaping the policies that affect their lives. Anticipatory governance and decolonial sociotechnical foresight can play a critical role in this context by equipping public institutions with the tools and frameworks necessary to learn from historical systematic institutions of inequality and foresee potential challenges and opportunities. By employing data-driven approaches and scenario planning, governments can better understand emerging trends and their implications for service delivery.

Foster multistakeholder partnerships: Encourage collaboration among diverse stakeholders, including government entities, private tech companies, civil society organizations, international development assistance (IDA) organisations, and academia, to adopt a sociotechnical participatory approach in developing innovative solutions for data management and protection. By engaging multiple perspectives and expertise, these partnerships can enhance the collective capacity to handle data securely while promoting economic growth, through collaborative frameworks that will ensure that data governance strategies are inclusive, addressing the needs and concerns of all stakeholders involved, and ultimately fostering a more resilient and equitable digital ecosystem. The public sector should create platforms for dialogue among stakeholders, including the tech community, and civil society, to discuss challenges and opportunities related to data governance and digital trade.

Invest in digital public infrastructure (DPI): Allocate resources towards enhancing digital infrastructure, ensuring accessible, affordable, and high-quality connectivity, foundational elements for digital transformation, access to digital public goods (DPGs), and facilitation of efficient intra-regional digital trade. Additionally, investing in digital infrastructure is essential for making open data widely accessible to researchers, entrepreneurs, and the public, within and between countries.

Internet access is the key to delivering public services to people. If the service is not affordable to most people, goals of leveraging digital transformation for development will not be met. Over the past decade new financing and technology, along with privatization and market liberalization, have spurred dramatic growth in information and communication technologies (ICTs) in many countries, which are increasingly recognized as essential tools of development, contributing to global integration and enhancing public sector effectiveness, efficiency, and transparency.

Regional Bodies (SACU, AU)

Harmonize regulatory frameworks: Regional bodies should work towards harmonizing legal frameworks across member states to reduce policy fragmentation, by establishing common standards for data protection and privacy that facilitate seamless CBDF, that also align with global standards. Regional bodies can leverage the AfCFTA Digital Protocol to create a unified digital market that supports cross-border data flows and enhances regional integration. To enhance digital trade within SACU:

- Member states should prioritize harmonizing their data governance policies and e-commerce strategies.
- Collaborative initiatives should be established to share best practices and resources.
- Continuous engagement with continental bodies like the AU will be essential for aligning national policies with continental goals.

Promote capacity building initiatives: Organize training and capacity-building programs for member states to enhance their understanding of data governance and digital trade, that encompass

trade and non-trade related aspects of CBDF to enhance public sector innovation and equip stakeholders with the necessary skills to implement effective policies.

Furthermore, capacity building of data curators in the public sector is needed to create effective national statistics systems (NSS) that collect and disseminate comparable statistics on access, use, quality, and affordability of ICT are needed to formulate growth-enabling policies for the sector and to monitor and evaluate the sector's impact on development.

Private sector

Co-create ethical solutions for data-based systems (DS): Beyond market incentives, tech companies and other early data economy incumbents in the private sector should prioritize the development of DS that adhere to ethical standards, respect human rights, and support sustainable digital transformation. This includes transparency in data usage and accountability for data innovations that support the public good.

Foster local DS innovation ecosystems: Foster local innovation ecosystems that are increasingly dependent on foundational DS by collaborating with other stakeholders in data ecosystems to create technologies that address their unique challenges. This can empower local stakeholders and enhance digital inclusion and create homegrown contextually relevant solutions. Furthermore, engaging communities in the open data process is also key to empowering them to participate in data initiatives that address their specific challenges. By incorporating local perspectives and needs, open data initiatives can stimulate social innovation and economic development while upholding individual rights and privacy will support open data practices that will enhance information flow and cultivate a culture of collaboration and innovation that benefits all stakeholders in the data-driven data economy.

Media and civil society

Raise public awareness: Media outlets and civil society should implement initiatives that focus on educating the public about data protection rights and the importance of secure data flows to build a culture of awareness and demand for robust data governance. This can include developing articles, videos, and infographics that simplify the complexities of data rights, promote digital literacy, and emphasize the benefits of strong data governance.

Investigate and report on digital issues: Investigative journalism should focus on the implications of data policies and practices, holding governments and corporations accountable for data misuse and breaches. Examples can include analysing government regulations and corporate policies to assess their alignment with data protection principles and identify loopholes, uncovering cases of data misuse, breaches, and exploitation through on-the-ground reporting and whistleblower accounts, interviewing diverse stakeholders including policymakers, industry leaders, civil society advocates, and affected communities, to name a few. Media outlets should provide ample space for these investigations and ensure they are widely disseminated to maximize impact.

By shining a light on complex issues surrounding data governance, media and civil society can hold powerful actors accountable and push for reforms that support just data value creation.

Academia and Think Tanks

Conduct research on inclusive data governance: Academic institutions and other orgnisations in the policy-knowledge ecosystem such as think tanks should prioritize comprehensive research initiatives to analyse the effectiveness of existing data governance frameworks. Initiatives can range

from establishing dedicated research centres focused on data governance that bring together multistakeholder transdisciplinary teams of experts in law, technology, sociology, and public policy. These centres can conduct in-depth studies to assess the current state of data governance across various sectors and recommend evidence-based improvements. The proposed centres can also employ comparative analyses of data governance frameworks from different countries and regions to identify best practices and lessons learned. This can help inform local adaptations that consider cultural and contextual differences.

Research initiatives should involve a diverse range of stakeholders, including government agencies, private sector representatives, and civil society organizations, in the research process. A collaborative approach will ensure that the research addresses real-world challenges, and incorporates multiple perspectives, to provide insights and recommendations based on public interest, evidence-based findings, ensuring that academic perspectives inform the development of data governance policies.

Lastly, academia and think tanks should disseminate research findings through academic journals, policy briefs, and public forums to raise awareness and inform ongoing debates about data governance, including through engaging the media and other stakeholders in these discussions to amplify the impact of public interest research.

Collaborate on policy development: Academic institutions and think tanks should actively engage with policymakers to ensure that research findings inform the development of data governance policies. initiatives can range from establishing policy advisory committees that include academic experts who can provide insights and recommendations on data governance issues to bridge the research-policy gap between academia and government, and facilitate the exchange of knowledge and expertise amongst stakeholders, participating in public consultations on issues related to data governance, and collaborating with policymakers to conduct impact assessments of proposed data governance policies, evaluating their potential effects on various stakeholders and the broader data economy.

Fostering networks among academic institutions, think tanks, policymakers, and industry stakeholders to promote ongoing dialogue and collaboration on data governance issues can facilitate knowledge sharing and the development of cohesive policy frameworks.

Official Development Assistance (ODA) and International Development Assistance (IDA)

Prioritize support for local data governance initiatives: ODA and IDA should focus on funding programs that enhance data governance frameworks across African nations, ensuring they are inclusive, equitable, and sustainable. This support should prioritize initiatives that foster regional collaboration, harmonize regulatory frameworks, and build local capacities (technical and policy) for data management and protection for thriving local data ecosystems

Prevent tied aid and encourage sustainable local innovation ecosystems: To avoid creating dependency on foreign aid, and foreign consultants, and experts, development assistance should be structured to prevent tied aid, which often restricts funding to the purchase of goods and services from donor countries. Instead, ODA and IDA should prioritize supporting the establishment of robust local innovation ecosystems, which involves investing in capacity-building programs that empower various local stakeholders to develop contextually relevant solutions and prevent “Aid oligopolies”. By fostering collaboration among local businesses, academic institutions, and civil society organizations, these efforts can enhance the development of homegrown technologies and an enabling policy environment that effectively address local challenges.

Additionally, investing in digital public infrastructure is crucial to facilitate efficient CBDF and promote digital trade. Such investments can enhance access to essential digital services and tools, especially in Least Developed Countries (LDCs), Landlocked Developing Countries (LLDCs), and Small Island Developing States (SIDS). By aligning ODA and IDA strategies with the specific needs of local contexts, these funds can play a transformative role in strengthening data sovereignty, enhancing economic development, and ensuring that digital transformation benefits all stakeholders in the region.

8. References

Aaronson SA (2018). Data is different: Why the world needs a new approach to governing cross-border data flows. CIGI papers no. 197. Centre for International Governance Innovation, Waterloo, ON

Aaronson, S. A., & Leblond, P. (2018). Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. *Journal of International Economic Law, 21*(2), 245–272.

Abrahams, L., Burke, M., & Hartzenberg, T. (2023). *Digital customs transformation for effective trade facilitation and revenue collection* (SARChI Industrial Development Working Paper Series WP 2023-02). https://www.uj.ac.za/wp-content/uploads/2021/10/sarchi-wp-2023-02-abrahams-l--burke-m--hartzenberg-t-february-2023.pdf

Agreement Establishing the African Continental Free Trade Area (AfCFTA). (2018). African Union. https://au.int/en/treaties/agreement-establishing-african-continental-free-trade-area

African Union (AU).(2014). Convention on Cyber Security and Personal Data Protection (Malabo Convention). https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

AU.(2019).Strategy for Gender Equality and Women's Empowerment. https://au.int/en/articles/au-strategy-gender-equality-and-womens-empowerment

AU.(2022). Data Policy Framework (DPF). https://au.int/en/documents/20220728/au-data-policy-framework

Ahmed, S. (2023a). *Data justice for an inclusive African Digital Single Market*. Medium. Retrieved from https://shamiraahmed.medium.com/data-justice-for-an-inclusive-pan-african-digital-single-market-e59f012c3d2

Ahmed, S. (2023b). *Facilitating an African Digital Single Market*. Data Economy Policy Hub. Retrieved from https://www.dataeconomypolicyhub.org/post/facilitating-a-pan-african-digital-single-market

Ahmed, S., Tobing, D. H., & Soliman, M. (2023). Why the G20 should lead multilateral reform for inclusive responsible AI governance for the Global South. https://www.dataeconomypolicyhub.org/items/why-the-g20-should-lead-multilateral-reform-for-inclusive-responsible-ai-governance-for-the-global-south

Ahmed, S., Chinembiri, T., Moyo, M., & Gillwald, A. (2021). Future of Work in the Global South (FOWIGS): Digital Labour, New Opportunities and Challenges (Working Paper). https://policycommons.net/artifacts/2195339/future-of-work-in-the-global-south-fowigs/2951701/

Appaya, M. S., Gradstein, H. L., & Haji Kanz, M. (2020). *Global experiences from regulatory sandboxes* (Fintech Note No. 8). Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/912001605241080935/Global-Experiences-from-Regulatory-Sandboxes

Appiah-Thompson, C. (2023). Contentious Biometric Voters Registration and Democratic Politics under COVID-19: The Myth of 'Social Distance' in an African State? [Preprint]. https://doi.org/10.32388/9MXB5L

Babalola, O. (2023). Data Protection Legal Regime and Data Governance in Africa: An Overview. In B. Ndemo, N. Ndung'u, S. Odhiambo, & A. Shimeles (Eds.), *Data Governance and Policy in Africa* (pp. 71–96). Springer International Publishing. https://doi.org/10.1007/978-3-031-24498-8_4

Banga, K., Macleod, J., & Mendez-Parra, M. (2021). Digital Trade Provisions in the AfCFTA: What Can We Learn from South-South Trade Agreements? *Supporting Economic Transformation (SET) Working Paper Series*. ODI, London.

Bank, W. (2022). Interoperability: Towards a Data-Driven Public Sector. https://policycommons.net/artifacts/3376737/interoperability/4175607/fragments/

Beyleveld, A., & Sucker, F. (2023). Regulating Cross-Border Data Flows Under the AfCFTA Protocol on Digital Trade: The What, Why, How, Where, and When. *SSRN*. https://ssrn.com/abstract=4437331 or http://dx.doi.org/10.2139/ssrn.4437331

Brown, E., & Piroska, D. (2022). Governing Fintech and Fintech as Governance: The Regulatory Sandbox, Riskwashing, and Disruptive Social Classification. *New Political Economy, 27*(1), 19–32. https://doi.org/10.1080/13563467.2021.1910645

Burri, M. (2017). The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation. *UC Davis Law Review, 51*, 65-133. https://ssrn.com/abstract=3067973

Burri, M., Callo-Müller, M. V., & Kugler, K. (2024). The Evolution of Digital Trade Law: Insights from TAPED. *World Trade Review, 23*(2), 190–207. https://doi.org/10.1017/S1474745623000472

Casalini, F., & González, J. L. (2019). Trade and Cross-Border Data Flows. OECD. https://doi.org/10.1787/b2023a47-en

Ciuriak, D., & Ptaškina, M. (2018). The Digital Transformation and the Transformation of International Trade. *RTA Exchange*. International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB). https://ssrn.com/abstract=3107811

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

Cuevas, A. (2013). Southern African Customs Union revenue volatility: Roots and options for mitigation. https://www.elibrary.imf.org/display/book/9781616353995/ch003.xml

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

Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016, January). Internet Fragmentation: An Overview. *World Economic Forum*.

Economic Community of West African States (ECOWAS). (2023). Experts validate ECOWAS E-commerce Strategy (2023 – 2027) and Implementation Plan. https://www.ecowas.int/experts-validate-ecowas-e-commerce-strategy-2023-2027-and-implementation-plan/

Ferracane, M., Makiyama.H.L., and van der Merel.,E. (2022). Digital Trade Restrictiveness Index (DTRI) Database. European University Institute et al. https://dti.eui.eu

Finck, M., & Mueller, M.-S. (2023). Access to data for environmental purposes: Setting the scene and evaluating recent changes in EU data law. *Journal of Environmental Law*, 35. https://doi.org/10.1093/jel/eqad006

Financial Stability Board (FSB). (2023).Stocktake of International Data Standards Relevant to Cross-border Payments. https://www.fsb.org/2023/09/stocktake-of-international-data-standards-relevant-to-cross-border-payments/

Gao, H. S. (2021). Data Sovereignty and Trade Agreements: Three Digital Kingdoms. *SSRN Scholarly Paper 3940508*. https://doi.org/10.2139/ssrn.3940508

GO FAIR .(2024). Fair Principles. https://www.go-fair.org/fair-principles/

González Morales, L., & Orrell, T. (2018). *Data interoperability: A practitioner's guide to joining up data in the development sector* (60 pp.). United Nations Statistics Division. https://doi.org/10.25607/OBP-1772

González, J. L. (2021). Trade and Cross-Border Data Flows. Organisation for Economic Co-operation and Development (OECD). https://doi.org/10.1787/7bc12916-en

Habich, E. (2022). FRAND access to data: Perspectives from the FRAND licensing of standard essential patents for the Data Act proposal and the Digital Markets Act. *IIC – International Review of Intellectual Property and Competition Law*, 53, 1343–1373. https://doi.org/10.2139/ssrn.4119834

Hlomani, H., & Ncube, C. B. (2023). Data regulation in Africa: Free flow of data, open data regimes and cybersecurity. In B. Ndemo et al. (Eds.), *Data governance and policy in Africa* (pp. 97–130). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-24498-8_5

Hummel, P., Braun, M., Augsberg, S., & Dabrock, P. (2018). Sovereignty and Data Sharing. *ITU Journal on Future and Evolving Technologies*, *1*(2). https://www.itu.int/en/journal/002/Pages/11.aspx

International Finance Corporation (IFC).(2024). Banking on women who trade across borders. https://www.ifc.org/content/dam/ifc/doc/2024/banking-on-women-who-trade-across-borders.pdf

International Telecommunication Union (ITU). Measuring digital development: Facts and Figures 2023. https://www.itu.int/en/ITU-D/Statistics/pages/facts/default.aspx

IT for Change. (2022). Cross-border 'Data Flow with Data Rights.Retrieved from:https://itforchange.net/sites/default/files/2208/Cross-Border%20%E2%80%98Data%20Flow%20With%20Data%20Rights%E2%80%99.pdf

Johnson, W. G. (2023). Caught in Quicksand? Compliance and Legitimacy Challenges in Using Regulatory Sandboxes to Manage Emerging Technologies. *Regulation & Governance, 17*(3), 709–725. https://doi.org/10.1111/rego.12487

Nkala, S., & Maswabi, G. (2022, July 12). How Africa can achieve data sovereignty. *The African*. https://www.theafrican.com/data-sovereignty-africa

Organisation for Economic Co-operation and Development (OECD), World Trade Organization (WTO), & International Monetary Fund (IMF). (2019). *Handbook on Measuring Digital Trade* (Version 1). Paris, Geneva, and Washington, D.C.: OECD, WTO, and IMF. https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade.html

OECD. (2022) Measuring the environmental impacts of artificial intelligence compute and applications: The AI footprint. https://www.oecd.org/en/publications/measuring-the-environmental-impacts-of-artificial-intelligence-compute-and-applications_7babf571-en.html

Pittet, F. T. (2022). African participation in WTO e-commerce negotiations: Policy positions and development issues. South African Institute of International Affairs (SAIIA). https://saiia.org.za/wp-content/uploads/2022/07/Policy-Insights-131tigere-pittet-FINAL.pdf

Schweitzer, F., Saccomanno, I., & Saika, N. (2024). The rise of artificial intelligence, big data, and the next generation of international rules governing cross-border data flows and digital trade. *The Global Trade Law Journal, 1(2), 14-45*.

Randall, D.A., R.A. Wood, S. Bony, R. Colman, T. Fichefet, J. Fyfe, V. Kattsov, A. Pitman, J. Shukla, J. Srinivasan, R.J. Stouffer, A. Sumi and K.E. Taylor, 2007: Cilmate Models and Their Evaluation. In:Climate Change 2007: The Physical Science Basis. Contribution of Working Group I to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change [Solomon, S., D. Qin, M. Manning, Z. Chen, M. Marquis, K.B. Averyt, M.Tignor and H.L. Miller (eds.)]. Cambridge University Press, Cambridge, United Kingdom and New York, NY, USA

Rattray, C. (2024). ITU's global event on emerging technology for connectivity: Accelerating digital transformation in LDCs, LLDCs, and SIDS. https://www.un.org/ohrlls/news/itu%E2%80%99s-global-event-emerging-technology-connectivity-accelerating-digital-transformation-ldcs

Southern African Customs Union (SACU). (2024). https://www.sacu.int/

Sebestyén, V., Czvetkó, T., & Abonyi, J. (2021). The applicability of big data in climate change research: The importance of system of systems thinking. *Frontiers in Environmental Science*, 9. https://doi.org/10.3389/fenvs.2021.619092

Sirimanne, S. N., & Adhikari, R. (2023). How to unlock women's potential in the digital economy. World Economic Forum. https://www.weforum.org/agenda/preview/893135f8-7bfe-4a77-bfec-7b9e54d740b4/

Sulla, V., Zikhali, P., & Cuevas, P. F. (2023). *Inequality in Southern Africa: An assessment of the Southern African Customs Union*. World Bank Group. http://documents.worldbank.org/curated/en/099125303072236903/P1649270c02a1f06b0a3ae02e57eadd7a82

United Nations Development Programme(UNDP). (2024). Small Island Digital States: How digital can catalyse SIDS development (New York: UNDP Global SIDS Team,2024)

UN Trade and Development (UNCTAD). (2016). Data Protection Regulations and International Data Flows: Implications for Trade and Development. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf

UNCTAD. (2018). B2C E-commerce Index 2018: Focus on Africa. https://unctad.org/system/files/official-document/tn_unctad_ict4d12_en.pdf

UNCTAD. (2019). Digital Economy Report 2019, Value creation and capture: Implications for Developing Countries. https://unctad.org/system/files/official-document/der2019_en.pdf

UNCTAD.(2020). What is at stake for developing countries in trade negotiations on e-commerce?: The case of the joint statement initiative. https://unctad.org/system/files/official-document/ditctncd2020d5_en.pdf

UNCTAD. (2021a). Technology and Innovation Report, Catching technological waves: Innovation with equity. https://unctad.org/system/files/official-document/tir2020_en.pdf

UNCTAD. (2021b). Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow https://unctad.org/system/files/official-document/der2021_en.pdf

UNCTAD. (2021c).The Least Developed Countries Report 2021. https://unctad.org/publication/least-developed-countries-report-2021

UNCTAD. (2023). Digital Trade for Development. https://unctad.org/system/files/official-document/dtd2023_e.pdf

UNCTAD. (2024). Digital Economy Report 2024, Shaping an environmentally sustainable and inclusive digital future. https://unctad.org/publication/digital-economy-report-2024

Universal Postal Union (UPU). (2022). 2022 Postal Development Report: Postal journey towards a sustainable future. https://www.upu.int/UPU/media/upu/publications/postalDevelopmentReport2022.pdf

Wechsler, M., Perlman, L., & Gurung, N. (2018). The State of Regulatory Sandboxes in Developing Countries. *SSRN Scholarly Paper 3285938*. https://doi.org/10.2139/ssrn.3285938

Wilkinson, M., Dumontier, M., Aalbersberg, I., et al. (2016). The FAIR Guiding Principles for Scientific Data Management and Stewardship. *Scientific Data, 3*, 160018. https://doi.org/10.1038/sdata.2016.18

Witting, J., and Kuipers, P. (2022). FRAND issues under consultation from different policy perspectives. https://www.twobirds.com/en/insights/2022/global/frand-issues-under-consultation-from-different-policy-perspectives

World Bank (2016). World Development Report 2016: Digital Dividends. Washington, DC. https://www.worldbank.org/en/publication/wdr2016/background-papers

Xiao, A., Xu, Z., Skare, M. *et al.* Bridging the digital divide: the impact of technological innovation on income inequality and human interactions. *Humanit Soc Sci Commun* **11**, 809 (2024). https://doi.org/10.1057/s41599-024-03307-8

Zieliński, M. F. (2017). *Regional integration and customs: Enhancing the role of customs* (WCO Research Paper No. 41). World Customs Organization (WCO). https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/research-paper-series/41-miroslaw-zielinski.pdf

Appendices

Appendix A: Summary of global data from 2010 to 2020 of Secure Internet servers per 1 million people

Table 3 is a summary of global data from 2010 to 2020 of Secure Internet servers per 1 million people.

Table 3: Secure Internet servers per 1 million people

	Country						
Year	Botswana	Eswatini	Lesotho	Namibia	South Africa	Sub-Saharan Africa	World
2010	4.3	4.55	0.49	6.67	51.5	3.64	186
2011	5.62	6.33	0.98	11.26	81.63	5.63	237.21
2012	9.19	8.1	0.97	29.53	141.86	9.86	322.65
2013	9.92	9.84	1.93	33.57	172.59	11.93	367.8
2014	17.7	18.65	1.91	43.25	221.12	15.37	446.6
2015	32.54	25.57	6.61	63.96	270.36	18.76	568.32
2016	46.76	25.38	8.4	79.63	914.09	67.73	1256.17
2017	62.87	39.95	19.35	121.38	9490.51	570.44	3487.37
2018	122.79	52.57	37.76	152.14	12126.62	725.9	6116.06
2019	194.42	91.48	60.21	149.59	14469.54	795.77	9899.25
2020	243.48	108.41	66.55	218.55	14546.1	788.87	11415.85

Source: World Bank

Appendix B: Key questions for a transversal policy approach to the data economy

Assessing the DPF provides critical insights into the challenges and opportunities of digital trade in Africa. By addressing the identified gaps and leveraging SACU's experiences, the AU can develop a robust and inclusive digital trade policy framework that promotes economic growth, regional integration, and global competitiveness for all African nations. Getting the foundations right is essential for a trusted, sustainable, and inclusive digital future, and requires policy attention to respond to the following crucial challenges

- **Connectivity and infrastructure:** How can we ensure accessible, affordable, and high-quality connectivity for everyone, forming the foundation for digital transformation? Additionally, how can we strengthen the resilience of digital technology value chains and ensure secure and reliable internet infrastructure?
- **Data and cross border data flows (CBDF):** In the digital age, data and cross-border data flows drive economic and social activity. How can we enhance data access and usage while protecting privacy, mitigating risks, and reducing policy fragmentation?
- **Data-bases systems (DS) such as AI and other frontier technologies:** As DS such as AI permeate various sectors—disrupting labour markets, transforming education, revolutionizing healthcare, and improving decision-making—how can we maximize its benefits while ensuring the safety, security, transparency, and accountability of AI systems? With ongoing advancements in quantum technologies, immersive experiences, and other emerging fields, what will the next significant AI development be?
- **Safety and security**: With the increasing interconnectivity of products, services, and infrastructure, how can we better manage their digital security to prevent cyberattacks? Furthermore, as people spend more time online, how can we address harmful phenomena such as cyberbullying, illegal content, misinformation and their impacts on mental health and social cohesion?
- **Measurement**: Comparable statistics on access, use, quality, and affordability of ICT are needed to formulate growth-enabling policies for the sector and to monitor and evaluate the sector's impact on development. How do we build a robust, comprehensive, and comparable evidence base to inform evidenced-based policy making for the data economy? Capacity to develop a range of metrics, indicators, and visualisations – including countries' digital performance, AI policies and trends, and broadband connectivity that aligns with global best practices.
- **Human rights and ethics**: How can we ensure that digital technologies, data practices, and AI systems respect human rights and adhere to ethical standards? What frameworks and guidelines are needed to protect individual rights, promote fairness, and uphold ethical principles in the rapidly evolving digital landscape.
- **Local agency and responsible innovation ecosystems**: How can we empower local communities to have greater agency in the digital transformation process? What strategies can be implemented to foster local innovation ecosystems, enabling communities to develop technologies and solutions that address their unique needs and challenges while contributing to the global data economy?
- **Public sector innovation and anticipatory governance**
  How can we enhance public sector innovation to proactively address emerging challenges and improve service delivery? What strategies can be implemented to foster anticipatory governance, enabling public institutions to adapt to changing societal needs while ensuring transparency, accountability, and citizen engagement in the decision-making process?

Glossary

Term	Description
Capabilities	Encompasses the skills, knowledge, and competencies that member states have developed to utilize digital technologies effectively, including the ability to manage digital infrastructure and protect data privacy.
Data Economy	A global digital ecosystem where data is collected, organized, and exchanged by various entities—such as individuals, businesses, and institutions—to create economic value, driving innovation and productivity.
Data Economy Enablers	Necessary components that facilitate digital trade, such as data governance, infrastructure, privacy protection, accessibility, and capacity building.
Data Governance	Institutions, regulations, and frameworks guiding how data is collected, processed, stored, and shared, ensuring data privacy and security are maintained.
Data Interoperability	Enabling integration across systems, applications, platforms, and devices to access, exchange, and cooperatively use data in a unified manner, involving legal, organizational, technical, and semantic interoperability.
Digital Capabilities	Skills, knowledge, and understanding that help individuals live, learn, and work in a digital society, including digital literacy, data and media literacy, and digital communication.
Digital Infrastructure	The physical and virtual systems (e.g., internet connectivity, data centers, telecommunications networks) that support digital transactions and communications.
Digital Trade	The sale or purchase of goods or services conducted over digital networks (e.g., the Internet), encompassing e-commerce, digital content streaming, online advertising, and cross-border services.
Endowments	Natural and acquired resources that SACU member states possess, which can support digital trade, such as technological assets, financial resources, and human capital.
Internet User	Defined by the International Telecommunication Union as anyone who has accessed the Internet from any location in the last three months, using any type of device (e.g., computer, mobile phone, digital TV, etc.).
Just Data Value Creation	The equitable and ethical generation, distribution, and utilization of data to promote inclusive economic and social benefits across generations, recognizing data as a crucial factor of production.