Chapter 1 - Unpacking digital sovereignty through data governance by Melody Musoni

1. Introduction

Discussions around digital sovereignty or data sovereignty are gaining momentum among policymakers across the globe. There is a general conception across different governments that whoever controls data, or the data infrastructure, controls the digital economy. Xi Jinping, the President of China, pointed out that '...whoever controls big data technologies will control the resources for development and have the upper hand' (Pottinger and Feith 2021). African countries are also noting with concern the level of foreign influence within their digital policy space, and have committed to self-manage and govern their data through common and clearly defined data guiding principles (AU 2022a). But what does this exercise of sovereignty in the digital space really mean? Which aspects of the concept of digital sovereignty matter to different countries and why? How does the debate on approaches to digital sovereignty shape digital policy and industrial policy?

One way that policymakers have addressed these questions was by introducing policy frameworks and laws to govern data. Some of the policies govern personal data, non-personal data, electronic commerce, critical information infrastructure, cybersecurity and digital rights. These policies are ways for governments to exercise their authority or sovereign powers over data, data infrastructures and cyberspace. What is also clear is that policies on digital sovereignty are also shaped by domestic national agendas, political priorities, interests, and perspectives. In this sense, some approaches to data are state-centred (case of China) while others rely on corporate self-regulation with a focus on national security (case of the United States of America (US), while yet others aim at the protection of individual rights and privacy (case of the European Union (EU)) (Falkner et al. 2022). It is also clear that there are competing models of data governance and countries vying to influence global digital governance are promoting their own model and leveraging it to further their soft power.

The scope of this chapter is to provide a comparative analysis of how different states and blocs interpret the concept of digital sovereignty through data governance. It will compare the data governance approaches of the US, EU, China, India and Africa (touching on the AU and specific African countries). We selected these specific countries and regions to reflect the major points of difference in how the digital sovereignty discourse is reflected in data governance. This research is based on qualitative research methods, including analysis of selected country official legal texts, government policies, draft policy frameworks, policy briefs and other works published in this field. We also conducted interviews with various stakeholders across the selected regions who are actively working on data governance and digital sovereignty issues. The chapter also discusses the implications of the existing digital powers (the US, China, and the EU, as well as emerging ones such as India) on the policy landscape in developing regions, especially Africa. The goal of this discussion is to highlight the implications of the digital sovereignty debate on data governance policies in different regions of the world, to understand what motivates these debates and to draw conclusions for international cooperation.

This chapter is divided into six sections. After this first introductory section, section 2 discusses the meaning of digital sovereignty and how this debate connects with data governance. It explores how the concept of digital sovereignty is understood by different countries/blocs, and why this has begun to impact policy debates around data governance within the selected regions. Section 3 discusses the exercise of sovereignty over personal data. Section 4 discusses how states exercise their sovereignty over non-personal data and the importance of interoperable guiding principles on data to make it easier to address common cross-cutting challenges. Section 5 draws from previous sections and discusses the strict form of digital sovereignty being data localisation. It explores what data localisation entails, the different approaches to data localisation adopted by countries and how they impact data flows. The final section draws some conclusions from the analysis and some initial recommendations for policymakers. Further recommendations for the EU can be found in Chapter 3 (see Teevan and Domingo 2023 in this report).

2. Data governance and digital sovereignty

The question of data governance has become increasingly central to discussions about digital sovereignty in recent years for a variety of reasons. This section of the chapter briefly discusses the motivating factors shaping digital sovereignty debates in different regions, and how this has impacted their different choices in terms of data governance. Data governance frameworks can define the boundaries of a state's sovereignty. However, certain approaches to digital sovereignty may be perceived in a negative way and cause strained relations between digital powers.

The United States: Rise of Big Tech, data extractivism and limited governance

The US plays an important role in the discussions around digital sovereignty despite it not having a clearly stated position on digital sovereignty (Wood et al. 2020). The practices of its government and US-based companies have directly contributed to how governments govern data. The US is the home to leading technology companies – Google, Apple, Facebook (Meta), Amazon and Microsoft (GAFAM). These companies dominate the domestic markets of Europe and Africa. According to Forbes, only Deutsche Telekom (a German company) made it onto the Forbes top 20 tech companies at number 19, while 12 US companies made it on that top 20 list (Forbes 2023; Ponciano 2019). These US multinational big tech corporations already exercise much control over the production, analysis, and trade of data. The words of Mark Zuckerberg "In a lot of ways Facebook is more like a government than a traditional company" (Foer 2017) are quite telling of the kind of influence that big tech has over not only data or data infrastructure but also the people and entities who use the data and related infrastructure. Big tech influence was well demonstrated in the Cambridge Analytica scandal that exposed how platforms can be used to influence politics and democratic processes. The scandal unearthed the unethical data practices of Facebook and how personal data was manipulated for political campaigns (Chang 2018).

What also exacerbated discussions around digital sovereignty were the revelations by Edward Snowden. The Snowden revelations on the US government's global surveillance program through its National Security Agency (NSA) (Macaskill and Dance 2013) were quite impactful in digital geopolitics. Several governments responded by requesting cloud providers to have local storage for data belonging to their citizens (McKenna 2016). Due to the number of US tech companies operating across the globe, the US is not particularly concerned about the local storage of data as it is still able to exercise control over these companies. Back in 2013, Microsoft challenged the powers of the US government under the Stored Communications Act (SCA) to access data which was hosted on a server in Ireland as it argued that the US government had no sovereign powers on foreign territory (Microsoft Ireland v US). The US government argued that it enjoyed extraterritorial powers in terms of the SCA and could instruct any service provider to access data wherever it was located.

In response to the legal complexities of this case, the US Congress quickly passed the US Clarifying Lawful Overseas Use of Data (CLOUD) Act. The CLOUD Act 2018 authorises US law enforcement to demand access to data held by US companies overseas. This means that due to the dominant position of US big tech, the US is able to exercise its digital sovereignty powers, such as criminal investigations, even outside its territory. Developments in the US have led to multiple rounds of negotiations over EU-US cross-border data transfers. For example, the EU-US Data Privacy Framework for managing data transfers between the EU and the US was challenged by privacy activist Max Schrems at the Court of Justice of the European Union (CJEU) and subsequently invalidated in 2020 (Schrems II). The EU's recent adequacy decision for the US might be challenged before the CJEU (NOYB 2022).

Ultimately, the US government exercises its sovereignty over data and data infrastructures by passing laws which permit US authorities to compel service providers to disclose data. For the US, data sovereignty is not just about having control over data residing within its physical borders. Instead, it extends to exercising authority over data remotely hosted on cloud servers in other regions if the cloud service provider or telco is from the US. These powers can leave service providers caught up in a compliance battle due to conflict of laws between jurisdictions and have major implications for the sovereignty of other countries and regions.

China: State-led approach to data

In 2010, China published a white paper which outlined China's approach to what it terms cyber sovereignty. The white paper emphasised that the internet in China is under the jurisdiction of Chinese sovereignty (China Internet Information Center 2010). Cyber sovereignty in China means the right it enjoys as a country to shape its own digital domains without the interference of foreign actors. The Chinese government has imposed wide-ranging measures to control the internet such as content filtering, removal of content and censorship through what is dubbed 'the Great Firewall' (Anderson 2012). People in China can only access online content that the Chinese Communist Party wants them to access. Any content which is considered a threat to the national security or the moral interests of Chinese people is automatically blocked.

This model allowed for the emergence of Chinese digital platforms (see Karkare 2023 in this report) that have in many ways replicated the data extractivism of US big tech, while the Chinese government has considerable access to the data collected by Chinese companies. The Chinese government has privileged access to all data that originates in China. The 2017 Cybersecurity Law requires companies to transfer all 'critical information' to state-run servers. The 2021 Data Security Law requires Chinese companies to provide access to data for national security review when the state submits a request for access to data. This law also has extraterritorial implications (Kokas 2022). This has played a role in driving fears in the West about the operation of Chinese companies abroad (for example, TikTok) and whether they are sharing user data with the Chinese government.

The European Union: The norms and standards setter

The EU focuses on the sovereignty of individuals and emphasises fundamental values such as human dignity, freedom, democracy, equality, the rule of law and respect for human rights (EC 2022a; EU4Digital 2021; EC 2021). The EU explicitly wants to be the leader in creating global norms and standards in the regulation and standardisation of digital technologies. Key to this has been the high standard of data protection contained in the General Data Protection Regulation (GDPR 2018), which is now being coupled with policies that aim to develop a common data market in Europe to spur innovation. The EU's approach to digital sovereignty focusing on individual rights is in sharp contrast to the Chinese state-centred approach.

Internationally, the EU hopes to capitalise on the so-called 'Brussels Effect', meaning the de facto process of unilateral regulatory globalisation of EU laws outside its borders via market processes (Bradford 2019). This has seen multiple countries across the world adopt data regulations based on or closely related to the GDPR. In order to respond to the growing influence of China as exercised via the Digital Silk Road and multilateral fora, the EU is now pushing for a coordinated 'Team Europe' approach to promoting its model of data governance, including notably through the Global Gateway Strategy and the Digital for Development Hub. Rather than continuing to rely exclusively on market mechanisms to facilitate the spread of GDPR-style regulation, the EU is thus increasingly offering technical support to countries in the Global South that are interested in developing data protection regulation. This is increasingly being offered as part of wider support to countries in developing their digital policies and national strategies on digital transformation.

Africa: A digital decider?

African governments are adamant about not being left behind in the digital revolution as has happened with the previous three industrial revolutions. Having control over data and technology is an important policy objective to ensure Africa's digital sovereignty. However, there is no common approach to achieving this objective and each country governs data differently (Teevan and Domingo 2022). One of the common concerns among African countries is the lack of home-grown digital products and tools. This is exacerbated by the fact that the African cloud market is dominated by foreign actors who host African data on foreign-based servers. In the end, African governments have little control over where African data is hosted or how the data is used. This is seen as weakening the digital sovereignty of African states. The fact that foreign tech companies can extract African citizens' data and commercialise it without sharing the benefits with Africa has alarmed policymakers who portray such activities as modern-day digital colonialism. Coleman defines digital colonialism as a modern-day 'scramble for Africa' where big tech companies extract, analyse and own user data for profit and market influence with nominal benefit to the data source (Coleman 2019). African leaders increasingly consider that location of data infrastructures is a strategic issue and there is a need for local data centres to host African data (Velluet and Beaubois-Jude 2021). If Africa does not spearhead the discussions around how African data is governed and how data governance frameworks align with its continental development needs, then foreign actors will shape its digital space to their advantage (Hofmeyer et al. 2022).

The AU Digital Transformation Strategy for Africa 2020 - 2030 (DTS) identifies the need for respect of data sovereignty by localising data through Africa's Data Center Infrastructure designed to host mission-critical servers and computer systems, with fully redundant subsystems. The DTS is supported by numerous continental entities and initiatives, including the Programme for Infrastructure Development in Africa (PIDA) which supports the development of regional and continental infrastructure, with a particular focus on ICT, transport and energy. Governments have demonstrated their political will to improve the digital economy, with Rwanda and Kenya as good examples of African countries that have invested heavily in the digital economy and in becoming major digital players on the continent. President Kagame of Rwanda has been instrumental in championing digital integration in Africa and founded Smart Africa. Rwanda has relatively warm relations with a variety of global actors and is a preferred African hub for innovators. The Smart Africa Alliance is a good illustration of the commitment made by African Heads of State and Government, with members having agreed to accelerate sustainable socio-economic development on the continent, ushering Africa into a knowledge economy through affordable access to broadband and usage of ICTs. Kenya, as a founding member of the Smart Africa Alliance is leading on digital economy development and has worked closely with the EU in developing its data protection framework. However, it seems to be relaxing its data protection to strengthen its relations with the US in the context of the US-Kenya Free Trade Agreement (Omino and Rutenberg 2021).

Yet African governments do not have the financial resources to independently self-fund much of their digital infrastructure. A lot of digital infrastructure projects in Africa are funded by foreign actors from China, the US and Europe. There is a concern that such countries may not be able to develop an independent approach to digital sovereignty (Wood et al. 2020). Over a period of 15 years since 2005, China invested $7.19 billion in Africa's digital infrastructure. Huawei for example has built the majority of Africa's 3G and 4G networks, Hikvision has rolled out surveillance cameras in Johannesburg and China Telecom is providing fibre optic networks across Africa. China also sponsors African citizens to undergo training and education in China (Gravett 2020). US big tech firms control much of the cloud computing infrastructure in Africa and US digital platforms dominate the digital economy in Africa as in much of the rest of the world. Through the Global Gateway Strategy, the EU and its member states have promised to invest up to €150 billion in Africa by 2027.

A number of analysts have highlighted the threat of growing digital colonialism in Africa due to the extractive practices of US big tech, together with growing Chinese influence through digital investments. The Ugandan think tank, Pollicy, identified nine forms of digital extractivism, including data extractivism, which they identify as originating with Western companies, but increasingly being adopted by local companies (Iyer et al. 2021). Gravett (2020) argues that China's influence in Africa is giving rise to digital neo-colonialism, a term which means the application of economic and political pressure by China through technology to control and influence how African governments act, while Husami argues that any country which signs up to China's version of the internet can expose its people to the same levels of control as those exercised in China (Husami 2022). The concern is that if African governments fail to advance their own values and interests with equal boldness, the 'China model' of digital governance may become the 'Africa model' by default (Gravett 2020). However, this may not make much of a difference for authoritarian regimes in Africa which already have a similar approach to the Chinese on data governance. Automatically making China into a bad-faith actor does not serve to correctly identify and address the problems of the proliferation of surveillance tools (Jili 2022). To argue that China will influence African countries to adopt its approach to digital sovereignty creates an impression that African governments lack the sovereignty to make decisions for themselves and have to wait either to adopt the 'China model' or the 'EU model'.

It is possible for African governments, as sovereigns, to import Chinese technologies without necessarily adopting the Chinese model of cyber sovereignty, including its model of data governance. This would require African countries to have adequate data protection laws and insist on compliance with domestic certification standards. South Africa is a good example of an African country which imports digital products, including from China. The law requires South Africa's telecommunications regulator to approve digital products before they can be used in the country (section 35 of the Electronic Communications Act[1]). On the other hand, the Information Regulator monitors compliance with the Protection of Personal Information Act. Any responsible persons or data controllers, including foreign tech companies operating in South Africa, are subject to these domestic laws. Unfortunately, most African countries still lack the necessary policy and regulatory frameworks and have limited technical capacities, which makes it easier for foreign players, like China, to impose their approach to digital sovereignty.

Instead of proposing narrow options for Africa, guided by whether it adopts the 'US', 'EU' or 'China' approaches, policymakers should start thinking of prioritising the needs of Africa and developing a unique approach fit for Africa's purpose. A 2018 New America study grouped countries into three broad clusters in terms of internet governance. One cluster being sovereign and closed, the second being global and open and the third being digital deciders. Digital deciders are countries which might decisively influence the trajectory of international processes (Wood et al. 2020). What this means is that if African countries were to come together and agree on a common approach to data protection (for example, through the Malabo Convention) or a common approach to non-personal data (for example, through the Agenda 2063, the AU Data Policy Framework, the Digital Transformation Strategy and African Continental Free Trade Area), then an 'African model' to digital sovereignty can emerge. Since Africa's 55 countries all have different approaches to data governance and different understanding of what digital sovereignty entails, it is difficult to identify 'an African approach' to digital sovereignty. However, due to the sheer size of Africa's untapped market and its young population demography, there is significant potential for Africa to be a critical driver in establishing principles around digital sovereignty. This of course would rely on cooperation and coordination among all African governments and institutions with the support of the private sector and ironically, foreign actors like the EU.

3. Policies on the protection of personal data

The protection of personal data is an important policy issue in the digital economy. Personal data usually refers to any information which can be used to identify a person directly or indirectly. Depending on the context, it can vary from genetic, mental, physical, physiological, cultural data, location data, identification numbers and names. The uses of personal data are endless and include using digital ID to gain access to e-government services, to participate in political processes such as voting, to make online purchases, to access financial services, et cetera. Big tech

[1] The Electronic Communications Act 36 of 2005.

companies have become notorious for their data extraction practices and surveillance capitalism. Surveillance capitalism occurs when big tech extract private human experience and use it as raw material for translation into behavioural data (Laidler 2019) and for research and development purposes to maximise profits (Matambo and Ugar 2022). The Cambridge Analytica scandal (Chang 2018) is a constant reminder of how big tech can manipulate our personal data.

Digital sovereignty over personal data can be viewed in two ways. First, it is the ability of individuals and communities to make decisions about their personal data, whereby consent plays an important role (Internet society 2022). An individual can exercise control over their personal data by consenting to the type of personal data which can be collected about them, how such personal data is processed, who the data is shared with and the activities that can be performed in respect of their personal data. This of course has raised questions around data ownership. Should the entity extracting and creating value out of the personal data own the data or should ownership remain with the data subject or individual to whom the data relates? This is a question still open for debate with some arguing that, personal data ownership is incompatible with a rights-based approach to personal data (World Bank 2021) and the right of access to the data is more important for companies than owning the data (Thouvenin and Tamo-Larrieux 2021; Douilhet and Karanasiou 2016; Jurcys 2020). Another important question is whether individuals as owners of data can sell their personal data to companies? This comes from the concerns that when individuals use free online services such as accessing free public wifi, or using freemium app services, they pay for it with their personal data (Elvy 2017; van Lieshout 2015).

Secondly, digital sovereignty can be viewed as efforts by governments to put in place laws and policies to protect personal data. Most of these data protection laws establish supervisory authorities who have the power to oversee how data controllers process data and enforce the law. Data controllers mean entities (private or public) responsible for determining the means and purpose of processing personal data. Some data protection authorities enjoy institutional and financial independence and are accountable only to a country's constitution and the parliament. Data protection laws affords individuals with certain rights such as right of access to their personal data, right to be notified about the processing of their personal data, right to rectify and correct any records of their personal data, right to object to the processing of their data and right to approach the courts or the supervisory authorities for legal recourse. These data protection laws give back the power and control over personal data to individuals and in limited and clearly defined situations to data controllers.

In the age of disruptive emerging technologies, it is equally important to frame policies and laws which can address the processing of personal data by emerging technologies such as artificial intelligence, big data analytics and facial recognition software. These technologies may collect excessive amounts of personal data and there is a need to update data protection laws. In the absence of policy frameworks to protect personal data, emerging technologies may be used to abuse personal data. The European Union, the data protection authorities of The Netherlands and France, and others sponsored a Global Privacy Assembly resolution on facial recognition. This resolution highlighted the importance of lawful, reasonable and proportionate use of such technologies guided by data protection principles (Global Privacy Assembly 2022).

Policymakers should work towards ensuring that new technologies are carefully regulated in line with data protection laws. In instances where there are loopholes in legal frameworks, there should be policy interventions to address such loopholes. In the following section, we discuss the different approaches to data protection in different regions. These approaches are discussed within the context of understanding digital sovereignty over personal data.

United States

The US does not have a comprehensive data protection regime. Lawmakers in the US have repeatedly failed to develop data protection regulation, despite growing concern about how American citizens' data is used and abused by private companies. A number of high-profile hearings in Congress with Mark Zuckerberg and others have failed to produce effects. Congress is also considering banning TikTok for lack of safety and privacy features on the platform to protect children (Paul 2023). However, the ban of TikTok may not solve the identified problems since other US tech companies use the same data collection techniques. In the meantime five US states have developed their own data protection regulations (California Consumer Privacy Act; Connecticut Data Privacy Act; Utah Consumer Privacy Act;l Virginia Consumer Data Protection Act; Colorado Privacy Act). A data protection law at the federal level may be the best way for the US government to protect personal data of all its citizens and residents.

In 2022, the US, together with other partners launched the Declaration of the Future of the Internet. One of the commitments in the declaration is the protection of individuals' privacy, their personal data, the confidentiality of electronic communications and information on end-users' electronic devices, consistent with the protection of public safety and applicable domestic and international law (Declaration of the Future of the Internet). The declaration has been criticised for being full of empty promises as it offers little to combat massive data collection and profiling by big tech (Access Now 2022) and some of the participating countries to the declaration do not have clean records on data protection and internet freedoms. For example, threats to digital freedoms in Colombia and use of spyware to target journalists in Hungary (Engler 2022).

China

China recently passed the Personal Information Protection Law (PIPL) and the Data Security Law in 2021. These laws have strict localisation measures on citizens' data (Rolf 2023). The PIPL is less about privacy and more about protecting personal data which can be deemed confidential, extending to what was already in place under the civil code. The DSL requires that business data be classified according to its relevance to national security and public interest. Companies wishing to transfer data outside of China must perform internal security review before applying for a security assessment and approval from the relevant authorities. EU and US businesses operating in China would need to comply with these requirements. One of the major challenges for EU/US businesses operating in China is conflict of laws, especially when it comes to cooperating with law enforcement authorities who may want to access data. For example, the DSL does not allow foreign law enforcement authorities to access data stored in China unless the Chinese authorities have approved (Article 36 DSL). This is in sharp conflict with the CLOUD Act which allows US law enforcement agents to access data regardless of where it is located. It is important for policymakers around the globe working on data governance issues to be strategic in how they approach this sensitive issue and provide recommendations which can ultimately respect the sovereignty of all countries while allowing criminal justice to take its course.

While there is an increase in greater protections for user privacy and data, the Chinese government is increasing its surveillance tools. The Chinese social credit system is an example of a powerful tool on data governance. If Chinese citizens have low social credit scores, they can end up being punished by various sanctions such as throttling of their internet speeds, banning them or their children from attending good schools or blocking them from using public transportation (Ma 2018).

European Union

The European Union has been leading in the protection of personal data, especially with the introduction of the GDPR. The GDPR applies directly to any processing activities of personal data of European citizens and residents. It sets out 7 key principles of lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity, and confidentiality; and accountability which must be complied with when processing personal data. The GDPR adopts a 'rights-based' approach where it recognises eight fundamental rights being, rights in respect of automated decision making and profiling, right to data portability, right to restrict processing, right to be informed, right of access, right to object, right to erasure and right to restrict processing. The European Union is determined to use its legal standards and institutions in becoming a global normative power in regulation. Some of its laws have the ability to become entrenched in legal and policy frameworks in other regions. This is referred to as 'the Brussels Effect' or 'Europeanisation' (Bradford 2012). The extraterritorial application of the GDPR means that entities outside EU/EEA all need to comply with the GDPR if they are processing data of European citizens and residents to avoid losing access to the EU lucrative market (Levin 2021; Voight and vom dem Bussche 2017; Albrecht 2016; Tankard 2016). The strict sanctions and fines have made the GDPR quite an important law to comply with. Several jurisdictions, including within Africa, have subscribed to the principles set out in the GDPR in developing their own data protection frameworks. Kenya, as an example, received support from the EU to develop its data protection law (Erforth and Martin-Shields 2022).

The GDPR places stringent requirements before personal data can be transferred outside the European Union region. Failure to meet these requirements can result in personal data not leaving the EU. The GDPR permits international data transfers based on an adequacy decision (Article 45). For the European Commission to pass an adequacy decision, it considers a variety of factors which includes whether a foreign state respects human rights and fundamental freedoms. Cross border transfers of personal data under the GDPR are also permitted if there are appropriate safeguards (Article 46). The GDPR provides that appropriate safeguards may be provided for by a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority and approved by the Commission, approved codes of conduct or approved certification mechanism. Apart from relying on the adequacy decisions and appropriate safeguards, the GDPR also permits cross border flow of personal data under specific situations (Article 49).[2] Recent developments have also indicated that these mechanisms would need supplementary security measures for them to work, which is making it increasingly difficult for companies to transfer data outside the EU (EDPB 2020).

While Europe and the US are working hard to improve the framework to allow for transatlantic data transfers (EC 2022b; EC 2022c), the EU has also started negotiations on similar bilateral frameworks with African governments. It is too early to assess the progress made in this regard. The EU should move from supporting a few countries in setting up their data protection authorities to a broader discussion regarding the future of EU-Africa data flows. These discussions are a priority and strategic for the EU-Africa relations in light of the development of the AfCFTA. If the EU wishes to benefit from the African Digital Single Market, it needs to take the issue of data transfers seriously and negotiate a framework with favourable terms permitting data transfers between the two economic blocks. Cross border data flows are important for Africa’s economy as they improve how African businesses improve their businesses and for individuals to have a wide range of services to choose from.

India

India’s drive towards greater data sovereignty was motivated by the Cambridge Analytica data breach where nearly half a million affected users were Indian (Wood et al. 2020). At home, Indian citizens' data was also at risk from unlawful processing through the Aadhaar system. The Aadhaar digital system or India’s National Unique Digital Identity system allows Indian citizens to voluntarily register their biometric data to receive e-government services. The Aadhaar system collects both fingerprint and iris scans and over a billion people are already using the system. There have been concerns that the Aadhaar system and the Aadhaar Act lacked the appropriate privacy protections (Rakesh 2016; Vismay 2019; Bhandari 2019). In 2017, the constitutional validity of the Aadhaar system was challenged. The Supreme Court of India recognised the right of privacy and imposed an obligation on the government of India to introduce a law to enforce the right to privacy of individuals (Justice KS Puttaswamy vs Union of India).

Consultations were held with various stakeholders and a process was set in motion for the development of India’s legislation on data protection. The Digital Personal Data Protection Bill, which was proposed by the Ministry of Electronics and Information Technology in 2022, still needs to be approved by the Indian Parliament after

[2] Article 49 of the GDPR provides that in the absence of an adequacy decision pursuant to Article 45 (3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place under certain conditions.

consultations ended in January 2023. The bill allows cross-border data sharing between India and selected countries, and also grants individuals the right to obtain information, seek correction and erasure. However, the bill does not differentiate sensitive personal data (ethnicity, racial, health information) from other personal data. In practice the former needs to be more protected to ensure the privacy of data subjects (Ray et al. 2022). Further, similarly as the EU's GDPR, the Digital Personal Data Protection gives data users more power over how their data is used, yet the government has greater control over data storage and processing than it is allowed under the GDPR. Under a government directive from 2022, the Indian Computer Emergency Team (CERT-in) ordered virtual networks, virtual private servers, cloud services and data centres to store user data for up to 5 years, thereby risking undermining data privacy rights. Human rights defenders and civil society organisations have raised concerns over their limited ability to make the government accountable for data privacy issues (HRW 2022). Having a data protection law in place is quite urgent for India especially considering the amount of personal data processed under the Aadhaar digital ID system.

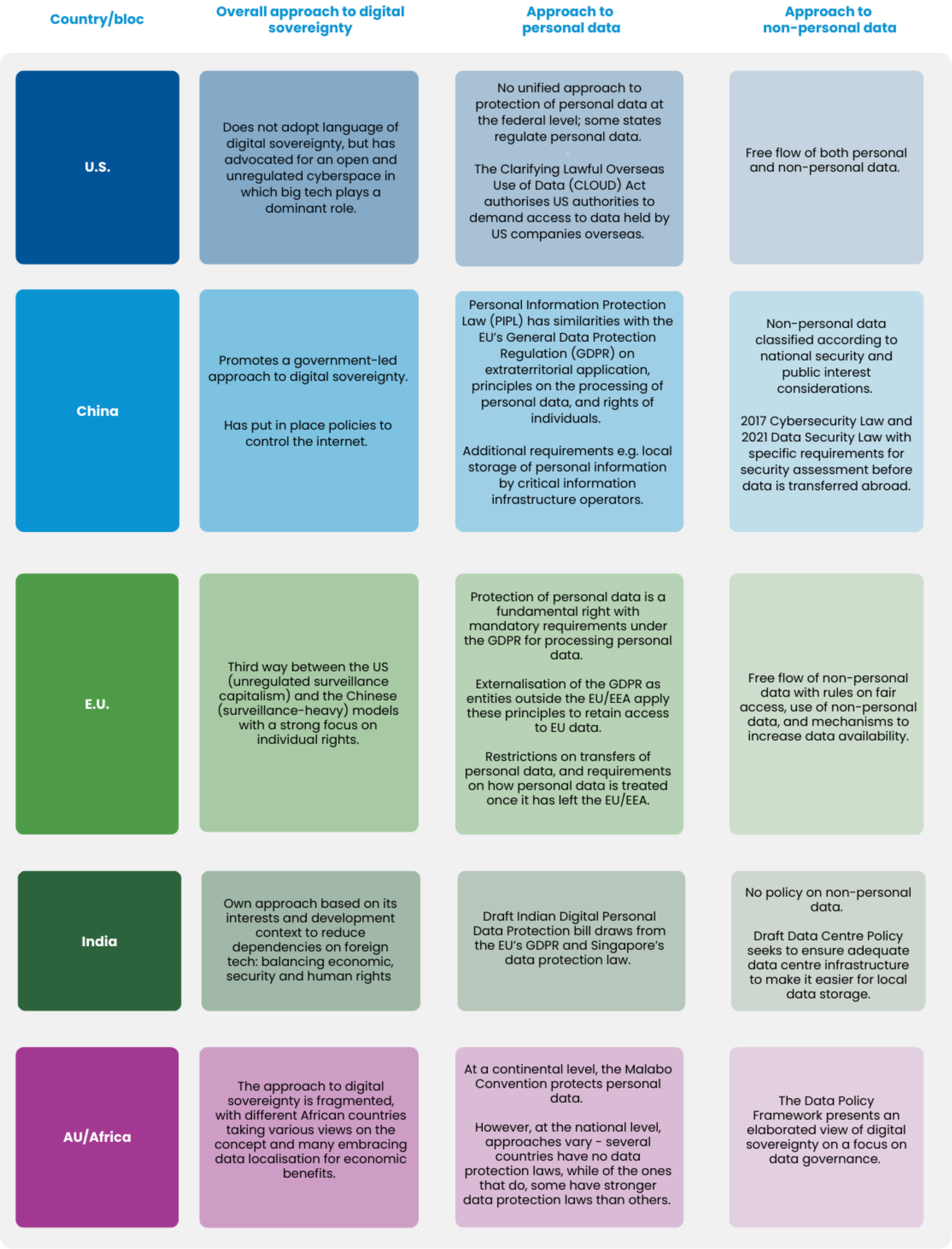
Africa

African countries also made efforts to regulate the processing of personal data. Different regional economic blocs have data protection frameworks (the 2008 East African Community Framework for Cyber Laws (EAC), the 2010 Supplementary Act on Personal Data Protection of the Economic Community of West African States (ECOWAS), and the 2013 Southern African Development Community model law harmonising policies for the ICT market in Sub-Saharan Africa (SADC)). Smart Africa is working with the Network of African Data Protection Authorities (NADPA) to map out legal frameworks, guidelines and recommendations on enhancing harmonisation and collaboration between data protection authorities among Smart Africa member states (Smart Africa 2022).

At a continental level, the AU seeks to regulate processing of personal data through the African Union Convention on Cyber Security and Personal Data Protection (AU 2014). The Malabo Convention was an attempt to address issues on data protection, electronic commerce, cybercrime and cybersecurity. The convention will come into operation once it has been ratified by 15 member states. At present, there are 14 ratifications (Status of the Malabo Convention 2023). However, the Democratic Republic of Congo recently announced its ratification, while the Gambia had previously announced its ratifications, bringing the total number of ratifications to 16 (Privacy in Africa 2023). It is not clear whether the Convention is not yet operational because these two countries are yet to deposit their instruments of ratification with the Chairperson of the AUC as required by Article 36 of the Convention. Already there are calls for the convention to be updated due to its inadequacies and misalignment with current policy developments and technological changes. The AU Data Policy Framework points out that the GDPR, APEC Privacy Framework and the Trans-Pacific Partnership Agreement may serve as points of reference for Africa's concerted efforts of data protection. In 2022, the AU advertised a call for a consultant to review the Malabo Convention and recommend additional protocols (AU 2022b). The amendment of the convention can be an opportunity for policymakers to advocate for more robust principles that would remove fragmentation hurdles, promote cooperation and the cross-border flow of personal data. As a way of bolstering relations, the EU should consider supporting the AU in updating the Malabo Convention by providing technical support and expertise based on its experiences in developing the GDPR. This support should not amount to recommending African leaders to copy and paste the GDPR, but would entail considering Africa's sovereignty, priorities and contexts and identifying important principles which should be included in the revised Malabo Convention or protocol.

Despite the challenges in having an operational convention at the AU level, member states have been promulgating data protection laws at domestic level. To date, over 60 percent of African countries have a law protecting personal data (Lovells 2023). These data protection laws cover important data protection principles, introduce data subject rights and appoint or create certain institutions, such as data protection authorities. This is quite an improvement. Between 2019 and 2022, there was a sudden increase in the number of data protection laws being passed on the African continent in countries like Botswana, Rwanda, Eswatini, Tanzania, Zambia and Zimbabwe. This might have been because of the growing awareness of data protection laws and increase in digitalisation as a result of Covid-19 pandemic.

Figure 1.1: Different approaches to governance of personal and non-personal data



Country/bloc	Overall approach to digital sovereignty	Approach to personal data	Approach to non-personal data
U.S.	Does not adopt language of digital sovereignty, but has advocated for an open and unregulated cyberspace in which big tech plays a dominant role.	No unified approach to protection of personal data at the federal level; some states regulate personal data. The Clarifying Lawful Overseas Use of Data (CLOUD) Act authorises US authorities to demand access to data held by US companies overseas.	Free flow of both personal and non-personal data.
China	Promotes a government-led approach to digital sovereignty. Has put in place policies to control the internet.	Personal Information Protection Law (PIPL) has similarities with the EU's General Data Protection Regulation (GDPR) on extraterritorial application, principles on the processing of personal data, and rights of individuals. Additional requirements e.g. local storage of personal information by critical information infrastructure operators.	Non-personal data classified according to national security and public interest considerations. 2017 Cybersecurity Law and 2021 Data Security Law with specific requirements for security assessment before data is transferred abroad.
E.U.	Third way between the US (unregulated surveillance capitalism) and the Chinese (surveillance-heavy) models with a strong focus on individual rights.	Protection of personal data is a fundamental right with mandatory requirements under the GDPR for processing personal data. Externalisation of the GDPR as entities outside the EU/EEA apply these principles to retain access to EU data. Restrictions on transfers of personal data, and requirements on how personal data is treated once it has left the EU/EEA.	Free flow of non-personal data with rules on fair access, use of non-personal data, and mechanisms to increase data availability.
India	Own approach based on its interests and development context to reduce dependencies on foreign tech: balancing economic, security and human rights	Draft Indian Digital Personal Data Protection bill draws from the EU's GDPR and Singapore's data protection law.	No policy on non-personal data. Draft Data Centre Policy seeks to ensure adequate data centre infrastructure to make it easier for local data storage.
AU/Africa	The approach to digital sovereignty is fragmented, with different African countries taking various views on the concept and many embracing data localisation for economic benefits.	At a continental level, the Malabo Convention protects personal data. However, at the national level, approaches vary - several countries have no data protection laws, while of the ones that do, some have stronger data protection laws than others.	The Data Policy Framework presents an elaborated view of digital sovereignty on a focus on data governance.

Source: Authors

4. Policies on the protection of non-personal data (industrial data)

Efforts by governments to exercise sovereignty or authority over non-personal data showcases the importance and the value of data. Data is a valuable strategic asset in a digital economy which is integral for planning, policy making, creating new opportunities for businesses and individuals and boosting the growth of the economy. Surprisingly, policymakers have acted oblivious to this and have taken a long time to implement policy frameworks and laws regulating data. With the increase in the use of big data analytics and artificial intelligence (AI), there is a growing need for rules, regulations and policy direction on how AI should be leveraged in a way that is beneficial to people. For African countries, it is important to have AI technologies which offer products and solutions beneficial to local markets. This calls for policy responses to AI which are based on national data governance frameworks, which promotes community participation and beneficiation, as well as advancing African value systems (Adams 2022). At the same time, there should be security measures in place to protect and safeguard this data from unwanted actors. In this section, we compare the data governance frameworks of Europe and Africa.

European Union

Having missed out on the platform economy, the EU is keen to ensure that European researchers and businesses are able to take advantage of the next phase of the data economy by creating a single market for non-industrial data. As a leader on regulatory policies, the EU is developing an arsenal of legal frameworks governing data. The 2018 Regulation on free flow of non-personal data demonstrated that the EU wants to ensure the free flow of industrial data (OJEU 2018). In 2020, the EU released its Data Strategy (EC 2020), which aimed to make the EU a leader in a data-driven society by creating a single market for data to allow the free flow of data for the benefit of businesses, researchers and public administrations.

The Data Act (still going through the legislative process) is a key pillar of the European strategy for data (EC 2022b). It addresses the sharing of non-personal data between businesses, ensures that a wider range of stakeholders gain control over their data and that more data is available for innovative use, while preserving incentives to invest in data generation. The Data Governance Act is another key pillar to the EU Data Strategy. It seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome obstacles to the reuse of data. It aims to facilitate the reuse of certain categories of protected data held by public sector bodies, it puts in place measures to ensure that data intermediaries will function as trustworthy organisers of data sharing as well as making it easier for citizens and businesses to make their data available for the benefit of society (OJEU 2022). The act came into force on 23 June 2022. GAIA-X is a notable initiative which aims at giving users sovereignty over their data by establishing an ecosystem whereby data is shared and made available in a trustworthy environment. The project was originally about creating a European cloud to rival US hyperscalers (AWS, Google, Microsoft), whereas it now appears to focus more on increasing competitiveness by holding everyone to the same standards and developing interoperability (Forrester 2022). Since GAIA-X was originally about the sovereignty of the EU, there was criticism levelled against the GAIA-X when it accepted sponsorships from Chinese companies to its 2021 summit as well as allowing foreign companies to participate in GAIA-X's technical working groups (Atlantic Council 2022).

Africa

The African Union, in an effort not to be left behind, recently published the AU Data Policy Framework, which is instrumental in the future of data governance on the African continent. Its purpose is to create an enabling policy environment for the private and public investments necessary to support data-driven value creation and innovation, collaboration between in-country sectors, institutions, and stakeholders, and harmonise policies across the continent in a manner that provides the scale and scope required to create globally competitive markets. The framework received financial and technical support from Germany's GIZ and South African think tank, Research ICT

Africa. The EU has invested €30 million in the EU-AU Data Governance initiative, which will be focused on the implementation of the framework by way of three pillars: data governance frameworks, data use cases and data infrastructure (Teevan and Domingo 2022; GIZ 2021).

Developing a common data market will be essential to support the roll out of the African Continental Free Trade Area (AfCFTA) Agreement and to build the Digital Single Market (DSM). If Africa creates the world's biggest DSM and invests in its technology industry, it can use that economic power and influence in norms and standards setting. Of course, there will be the concern of whether African norms will be enforced globally like the EU norms especially considering the existing 'hierarchy of sovereignty' where African voices keep being dismissed on international fora and the 'West's claim to the moral high ground' (Tadesse Shiferaw 2023).

The cases of Rwanda and South Africa can demonstrate some of the differences in how African governments approach the issue of digital sovereignty. In Rwanda, the Data Revolution Policy provides a framework for various key players to coordinate and work together (Republic of Rwanda 2017). This extends to establishing a national data office consisting of highly skilled experts in the data science field to coordinate the rest of stakeholders and drive the implementation of data revolution policy. The Rwanda Data Revolution Policy also establishes a national data portal which shall be managed by the data management body under the National Institution of Statistics and shall be responsible for providing structured and unstructured sets collected from all government and private sector agencies.

South Africa's draft data policy on the other hand focuses more on data ownership, with the government being the custodian and owner of all data generated in South Africa. The policy promotes localisation of government data as well as keeping copies of personal data for ease of access by law enforcement. The policy proposes the development of an open data strategy/framework for the sharing of data, informed by Data for Good principles, to enable access to relevant data for all South Africans. This draft policy has received several criticisms due to its vague and sometimes incorrect references to data-related concepts and terminology (Razzano 2021; van der Berg 2021).

A common approach to data governance can help African governments enjoy their sovereignty while also benefiting from data shared from other countries. Policymakers need to think carefully about how this framework can be adopted and implemented at domestic level. Guiding principles in the framework may not be easily translated in domestic laws. This may be because of the differences in national laws on data protection, data strategies and cybersecurity. As a result, there will not be data policy interoperability which can potentially frustrate the use and sharing of data in Africa. The AU Data Policy Framework provides a common ground for AU member states to implement the guiding principles at domestic level.

5. Policies on data localisation

The provision of cloud services is of strategic importance in the digital sovereignty debate. Factors such as the location of data or data centres, the national origin of the cloud service providers, the rules around access, sharing and processing of such data all influence the geopolitical tensions around digital sovereignty. Governments across the world approach data localisation from different perspectives and their varied interests influence their approach to data localisation. The underlying common understanding is that national sovereignty is threatened if governments are unable to exert full control over cross border stored data.

The following section discusses data localisation measures as tools used by governments to exercise digital sovereignty over data created within their jurisdictions and personal data of their citizens and residents. It discusses the different motivations for data localisation by selected countries. This discussion is meant to point out the lack of evidence to support certain data localisation policies, highlights the unintended consequences of certain forms of data localisation and emphasises the need for a common approach to data governance among like-minded governments. It is not the scope of this chapter to discuss in detail the economic, political and social impacts of data localisation. We discuss the policy implications of data localisation within the framing of the digital sovereignty discussion.

What is data localisation?

There is no single or official definition of data localisation. Fraser defines data localisation as the laws or measures put in place by governments which encumber the movement of data across national borders or limit where and by whom they are stored or processed (Fraser, 2016). Chander defines data localisation as a second-generation internet border control which seeks not to keep information out but rather to keep data in (Chander 2015). The AU Data Policy Framework defines data localisation as involving the artificial erection of legislative barriers to data flows, such as through data residency requirements and compulsory local data storage. By 2021, about 62 countries had enacted data localisation requirements with China, India, Russia, and Turkey requiring forced data localisation (Dascoli 2021). Some point out that when discussing data localisation, it may be necessary to clearly distinguish between exclusive data localisation requirements and non-exclusive data localisation requirements (Svantesson 2020).

Policymakers have divergent views on data localisation. A country's approach to data localisation is determined by a myriad of factors such as the underlying policy objectives, existing legal environment, or targeted sectors (health, telecommunications, banking, insurance, et cetera) (López González et al. 2022). As global geopolitical tension worsens and as governments struggle with the power of foreign tech companies, data localisation presents itself as a justifiable measure to ensure governments continue to exercise sovereignty over data.

Those who favour data localisation view sending data abroad as increasing citizens' vulnerability to serious security issues and threats from foreign actors. The long arm of the US government has caused governments to work towards maintaining their national sovereignty over data and data infrastructures within their borders. Protection of privacy and the rights of citizens have also been reasons cited for adopting data localisation measures (López González et al. 2022). When data is stored abroad, there are legitimate privacy concerns especially if the recipients of the data are located in a country without adequate data protection laws or if they are not subjected to contractual obligations to comply with data protection rules (Gonzalez et al. 2016; Kuner 2014; Chen 2015). However, measures meant to protect citizens may result in the exact opposite as governments end up increasing their ability to surveil citizens, infringe on their freedom of speech, freedom of expression and right to privacy.

Both democratic governments and authoritarian regimes cite national security interests as a reason to tighten control of their national digital infrastructure through data localisation (López González et al. 2022; Yayboke et al. 2021). There is fear that if infrastructure (cloud infrastructure or telecommunications infrastructure) is controlled by a foreign government, it can access data that passes through the infrastructure (Wu 2021). Interestingly, policies driven by national security interests are not supported by evidence while others exaggerate the national security concerns. Unfortunately, strict data localisation requirements make it difficult for law enforcement agencies to cooperate and exchange information while also weakening intelligence-gathering networks (Yayboke et al. 2021).

Some governments argue that investment in local servers and data centres can boost the local economy and provide employment opportunities for citizens. Data localisation measures are seen as a way of developing domestic capacity and providing a competitive advantage to local companies amid the globalisation of the digital economy (Fraser 2016; López González et al. 2022). However, evidence shows that data localisation measures increase the costs of data hosting by 30 - 60 % (Wu 2021). Instead of creating opportunities for the local players, such measures actually hurt local economies.

Approaches to data localisation

There are generally three main types of data localisation requirements. These range from strict requirements, conditional measures to open data transfers. Strict data localisation measures typically entail the total ban on transferring data abroad or a requirement for local storage or processing of data (Bailey and Parsheera 2018). These restrictions can manifest in the form of policy, standards, laws, and regulations. In other instances, the restrictions come in the form of technical efforts aimed at the technical and physical architecture of the internet. For instance, Germany had planned to have its own data centres and re-route email traffic to avoid surveillance from the US (Hon et al. 2016). Whilst Germany's plans did not come to fruition, countries like China have been successful in controlling the physical infrastructure through which internet traffic is exchanged (Mishra 2019). Some restrictions can also focus on specific industry sectors. For example, Nigeria has strict localisation laws in respect of its telecommunications and ICT industry,[3] Ethiopia also imposes strict data localisation requirements in respect of domestic payment information, payment switch and ATM transaction data,[4] and Rwanda also has similar restrictions.[5] Russia's law also imposes local storage and processing of data.[6]

The second approach to data localisation are conditional measures. Conditional data localisation measures permit the transfer or processing of data outside a country under clearly defined conditions. These measures are prevalent in data protection laws in the sense that the conditions on data transfers can potentially create barriers to cross border data transfers to such an extent that they are effectively data localisation requirements. The GDPR is a good example of a law with *de facto* data localisation measures (Cory and Dascoli 2021) and compliance with the conditions may be very costly to the extent that some entities are forced to store data locally by default (Kugler 2021).

The third approach to data localisation are open data transfers. An open data transfer regime requires minimum regulatory burden to movement of data. Open data transfers occur where there are no barriers to the flow of personal data (Kugler 2021; Beyleveld 2021). Under this regime, processing of data can take place abroad. López Gónzalez *et al.* points out that there is a new category of data localisation emerging whereby states do not require local storage of data, but service providers guarantee access to data when required by regulators. For instance, Mexico's Federal Telecommunications Law requires data to be made available for 12 months, without stipulating that it must be stored in Mexico (López González et al. 2022).

The following section discusses the different data localisation approaches adopted by the US, China, EU, India and Africa. The polarised debate on data flows has serious implications. It is not the intention of this chapter to discuss in detail what these implications are. Instead, this chapter aims to highlight the role of data localisation measures in the discussion on digital sovereignty.

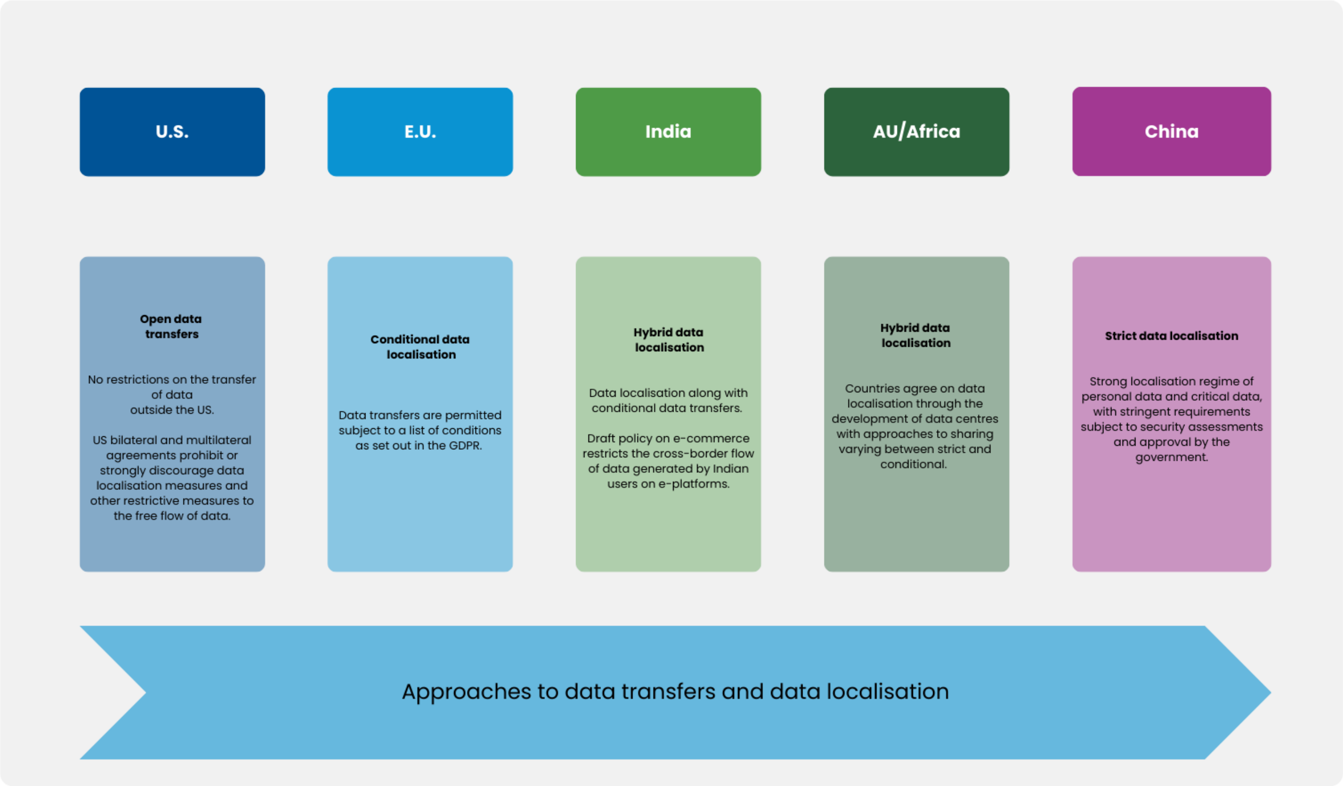
[3] Nigeria's Guidelines for Content Development in ICTs.

[4] The Licensing and Authorisation of Payment System Operators Directive No. ONPS/02/2020.

[5] Regulation No. 02/2018 on Cybersecurity.

[6] Federal Law No. 242-FZ.

Figure 1.2: Approaches to data localisation



U.S.

Open data transfers

No restrictions on the transfer of data outside the US.

US bilateral and multilateral agreements prohibit or strongly discourage data localisation measures and other restrictive measures to the free flow of data.

E.U.

Conditional data localisation

Data transfers are permitted subject to a list of conditions as set out in the GDPR.

India

Hybrid data localisation

Data localisation along with conditional data transfers.

Draft policy on e-commerce restricts the cross-border flow of data generated by Indian users on e-platforms.

AU/Africa

Hybrid data localisation

Countries agree on data localisation through the development of data centres with approaches to sharing varying between strict and conditional.

China

Strict data localisation

Strong localisation regime of personal data and critical data, with stringent requirements subject to security assessments and approval by the government.

Approaches to data transfers and data localisation

Source: Authors

United States: Open data transfers

The United States does not have a strict policy on localisation of data. Its tech companies and cloud service providers can host data anywhere in the world. In 2020, the US entered into a multilateral agreement with Canada and Mexico. This agreement prohibits data localisation and instead promotes the free flow of data between the countries.

As far as transfer of data for law enforcement purposes, the US laws permit US law enforcement authorities to access data held by US companies regardless of where it is located (CLOUD Act). However, the same CLOUD Act does not allow foreign governments to unilaterally access data stored on US soil. The growing geopolitical tension between the US and China has a direct impact on how Chinese companies operating in the US are treated. The US Congress recently summoned the CEO of TikTok to explain how the platform uses data. US officials are concerned that the user data could be accessed by the Chinese government and the platform can be weaponised by China to spread misinformation (Zahn 2023). Security experts have argued that there is lack of evidence that China has compelled TikTok to share user data (Zahn 2023). To allay the fears of Washington that Beijing can access user data, TikTok proposed for local data storage of US user data under the control of US companies through Project Texas. The Project Texas proposal signifies that data residency and storage location is very strategic for a country's exercise of data sovereignty.

While the US government may still prefer an open and free flow of data landscape, the attitude of its trading partners, allies and enemies may cause it to re-think its strategy. For example, the ban of EU-US data transfers in the Schrems I and Schrems II court cases has suspended personal data transfers from the EU to the US. If the current draft EU-US Adequacy Decision is not approved, US companies may be left in a dire situation which may force the US government to reconsider its approach to free flow data transfers and data protection law.

China: Strict data localisation

China on the other hand insists on strict data localisation which is the opposite of the US' open data transfers. Provisions of its Cybersecurity Law makes it mandatory for critical information infrastructure operators to store personal information and important data generated from critical information infrastructure in China.

Under its Data Security Law all businesses operating in China are required to store select data (for example, Chinese citizens' personal data) on servers within China. Where a transfer of locally stored data to another country is necessary, the Chinese government conducts a security assessment. The law also allows the Chinese government to conduct spot-checks on foreign businesses (Liu 2021).

European Union: Conditional data transfers

As mentioned earlier, the European Union's GDPR is a form of conditional approach to data localisation. Chapter V of the GDPR contains a list of conditions which must be met by a data controller or data processor before they can transfer data outside the EU. We have discussed the conditions for transfer of personal data in the section above.

The 2018 Regulation on free flow of non-personal data defines data localisation requirements as 'any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement, without prejudice to Directive 2014/24/EU, which imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State'. The regulation clearly states that the effective functioning of data processing and development of the data economy in the EU is hampered by data localisation requirements, as well as vendor lock-in practices[7] (OJEU 2018).

The EU also introduced the 2021 EU Cloud Code of Conduct (CCoC), which only grants permission to cloud service providers to operate cloud services in the EU if they follow certain requirements to protect personal data in accordance with article 28 of the GDPR. The code is the first of its kind. Alibaba Cloud, Google Cloud, IBM, and Microsoft have each implemented data protection provisions so as to comply with the code (Bendiek and Stuezer 2022).

India: Hybrid data localisation

India's approach to data localisation has evolved over the past years as the country has sought to balance security, economic as well as privacy concerns. The Indian government views data localisation requirements as a necessity to respond to foreign companies generating revenue from data of the Indian citizens (Wood et al. 2020). Based on the vision of 'Atmanirbhar Bharat' (loosely translated as a self-reliant India) and under the draft Data Centre Policy there are plans to increase India's data centre capacity, which is considered important for national security, economic growth and internet infrastructure.[8] The 2011 IT Rules impose requirements on the collection and disclosure of sensitive personal data in the private sector (Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules).

There have also been changes in India's approach to data localisation. In its previous version of the Data Protection Bill, India insisted on data localisation. However, Chapter IV of India's Digital Personal Data Protection Bill 2022

[7] Vendor lock-in occurs when a service provider supplies a customer with a product or service which is not compatible with those of competitors making it difficult for a customer to change service providers.

[8] India has currently over 138 data centres focused on cloud. The government aims to create four data centre economic zones to expand India's nascent data centre market, by attracting investment of $40 billion in the coming five years and putting economic incentives for businesses to construct data centres in the country. The increase in data consumption and generation by over billion digital users, will contribute to the growth of the value of the market $10.09 billion by 2027.

permits data transfers after an assessment by the central government. The central government may notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified. India's draft policy on e-commerce restricts cross border flow of data generated by Indian users on e-platforms (Government of India 2019).

Africa: hybrid data localisation measures

Africa is not in a dominant position of geopolitical power. Insisting on data localisation measures is its way of asserting sovereignty over data. Policy conversations regarding data residency on the African continent have frequently centred on localisation as a governance mechanism (Razzano 2021). A lot of African governments, as reflected by the language of the AU Data Policy Framework seek to gain control over the processing and utilisation of data generated on their territories. Africa only hosts 2% of the global data centres. There are nearly 50 data centres in Africa, five in Kenya, eleven in Nigeria, five in Morocco and twenty-five in South Africa (Resha 2021).

Lack of data centres on the African continent to host data of Africans is an important issue for African governments. There are legitimate fears that if diplomatic relations are strained between a government and the country where its data are hosted, the African country may be left in a vulnerable position. There is a concern that when African countries host data outside their borders, they cede political, economic and digital sovereignty to foreign powers (Velluet and Beaubois-Jude 2021; Domingo and Tadesse Shiferaw 2022). These legitimate concerns require urgent attention, and the guidance provided in the DTS and AU Data Policy Framework may be a good starting point. The DTS emphasises the need for local data centre infrastructure designed to host mission-critical servers and computer systems, with fully redundant subsystems. Having local data centres hosting government data helps African governments retain sovereignty over such critical infrastructure and information. Senegal has contracted Huawei to build the region's largest data centre, and all government data and digital platforms from foreign servers will be moved to the new data centre (Adegoke 2021).

The Smart Africa Alliance is also dedicated to ensuring that data centres hosting African content are built on African soil. For example, Djibouti is leading the Smart Africa flagship on construction of data centres on the African continent. Hosting African content on African soil will also reduce the cost of the internet and improve the quality of network signal.

Data localisation laws have an impact on cross border data flows (Mishra 2019), thus having an implication for African countries that seek to promote cross border data flows. Transborder data flows are regulated differently depending on whether it is personal data or non-personal data. Data protection laws of Rwanda and South Africa permit the transborder sharing of personal data subject to certain conditional requirements. As mentioned earlier, Rwanda only imposes strict data localisation requirements in respect of specific industries or sectors (like the finance sector). Its National Data Revolution Policy 2017 embraces the principle of national data sovereignty without insisting on data localisation. South Africa on the other hand leans towards a stricter approach to data localisation. The South African government has reiterated its concerns over South Africa's cloud computing infrastructure (data centre) investment being mostly foreign owned, having locally generated data being stored in foreign lands and Africa being an unequal participant in the global cloud market. To exercise its data sovereignty over cloud data, South Africa's policy provides that data generated in South Africa are the property of South Africa, regardless of where the technology company is domiciled. South Africa's draft Cloud and Data Policy reflects this and highlights data localisation as a policy objective, though it has been met with criticism due to unclear policy objectives and non-alignment with legal rules (Razzano 2021; Beyleveld 2021; Kugler 2021).

6. Conclusion

Our comparative analysis of the approaches to digital sovereignty by different regions and countries has highlighted a few important points which can help the future of digital policy. There is no ‘one size fits all’ approach to digital sovereignty. Each country has its own unique social, economic and political environment and technological capabilities which subsequently shape its domestic priorities and digital foreign policy. At the same time, some countries may not have clear cut approaches to digital sovereignty. To benefit from the digital economy, it is important for states to share data despite their approach to digital sovereignty. This means that instead of wanting to push one approach to digital sovereignty, policymakers need to create guiding principles on data which align with Sustainable Development Goals. They need to carefully navigate the differences between countries and provide policy recommendations which are beneficial to all (from human rights protection to economic benefit) while also respecting the individual sovereignty of each country.

Policymakers among like-minded governments such as the US and the EU member states should work towards developing policy frameworks which promote cooperation instead of competition. They need to adopt a multilateral approach, working with partners across the world to develop a new data governance approach which creates guiding principles on data processing, data transfer, data sharing as well as data access for law enforcement purposes. Such policies should adopt less restrictive measures, such as conditional data localisation in respect of personal data and open data transfers in respect of non-personal data. Policymakers can assist governments in developing clear guidelines on data localisation which promote digital inclusion, facilitate trade, preserve the sovereign interests of states and emphasise cybersecurity measures to ensure that data is secure, regardless of location.

Data governance frameworks play a crucial role in the exercise of digital sovereignty. In addition to this, certain industrial policies also shape a country’s approach to digital sovereignty. In the next chapter (Karkare 2023), we explore these industrial policies and how they shape a country’s approach to digital sovereignty. In the last chapter (Teevan and Domingo, 2023), we look at the policy implications of the different iterations of digital sovereignty in Europe and Africa and how that impacts the EU-Africa relations.

References - Chapter 1

Access Now. 2022. Empty promises? Declaration for Future of the Internet is nice on paper. Access Now.

Adams, R. 2022. AI in Africa: Key concerns and policy considerations for the future of the continent. Berlin: Africa Policy Research Institute.

Adegoke 2021. The real reason China is pushing "digital sovereignty" in Africa. Rest of World.

Albrecht, J.P. 2016. How the GDPR Will Change the World. European Data Protection Law Review, 2, 287-289. New York: HeinOnline.

Anderson, D. 2012. Splinternet Behind the Great Firewall of China: Once China opened its door to the world, it could not close it again. Volume 10, Issue 11 (November 2012), pp.40–49. Queue Magazine.

Atlantic Council. 2022. Washington DC. Digital sovereignty in practice: The EU's push to shape the new global economy'. Atlantic Council.

AU. 2014. African Union Convention on Cyber Security and Personal Data Protection. Addis Ababa: African Union.

AU. 2022a. AU Data Policy Framework. Addis Ababa: African Union.

AU. 2022b. Consultancy Services to Review the Malabo Convention on Cyber security and Personal Data Protection and Recommend Possible Amendments to Articles. Addis Ababa: African Union.

Bailey, R. and Parsheera, S. 2018. Data localisation in India: Questioning the means and ends. National Institute of Public Finance and Policy.

Bendiek and Stuezer 2022. 'Advancing European internal and external digital sovereignty'. Stiftung Wissenschaft und Politik.

Beyleveld, A. 2021. Data Localisation in Kenya, Nigeria and South Africa: Regulatory Frameworks, Economic Implications and Foreign Direct Investment. Policy Brief 7. Johannesburg: Mandela Institute, School of Law, University of The Witwatersrand.

Bhandari, V. 2019. Why Amend the Aadhaar Act Without First Passing a Data Protection Bill? Delhi: The Wire.

Bradford, A. 2012. The Brussels Effect. Northwestern University Law Review, Vol. 107, No. 1. Columbia Law and Economics Working Paper No. 533. New York: HeinOnline.

Bradford, A. 2019. The Brussels Effect: How the European Union Rules the World. New York: Oxford Academic.

Chander, A. and Uyen, P. 2015. Data nationalism. Emory Law Journal.

Chang, A. 2018. The Facebook and Cambridge Analytica scandal, explained with a simple diagram. Vox.

Chen, J. 2015. Data sovereignty, cybersecurity, and challenges for globalisation'. Georgetown Journal of International Affairs.

China Internet Information Center. 2010. V. Protecting Internet Security. Beijing: China Internet Information Center.

Coleman, D. 2019. Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. Volume 24. Michigan. Journal of Race and Law. Vol. 24.

Cory, N. and Dascoli, L. 2021. How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Washington DC: Information Technology & Innovation Foundation (ITIF).

Domingo, E. and Tadesse Shiferaw, L. 2022. The African Union at twenty: A new leader in digital innovation? ECDPM Commentary. Maastricht: ECDPM.

Douilhet, E. and Karanasiou, A. 2016. Legal Responses to the Commodification of Personal Data in the Era of Big Data: The Paradigm Shift from Data Protection towards Data Ownership. Effective Big Data Management and Opportunities for Implementation.

EC. 2020. The European Data Strategy. Brussels: European Commission.

EC. 2021. Global Gateway. Brussels: European Commission.

EC. 2022a. Declaration on European Digital Rights and Principles. Brussels: European Commission.

EC. 2022b. European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. Brussels: European Commission.

EC. 2022c. Questions & Answers: EU-U.S. Data Privacy Framework, draft adequacy decision. Brussels: European Commission.

EDPB. 2020. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021. Brussels: European Data Protection Board.

Elvy, S-A. 2017. Paying for Privacy and the Personal Data Economy. Vol. 117, No. 6. Columbia Law Review.

Engler, A. 2022. The Declaration for the Future of the Internet is for wavering democracies, not China and Russia. Washington DC: Brookings.

Erforth, B. and Martin-Shields, C. 2022. Where Privacy Meets Politics: EU–Kenya Cooperation in Data Protection. In: Africa–Europe Cooperation and Digital Transformation [Eds. Daniels, C., Erforth, B. and Teevan, C.]. London: Routledge (Pubs). London: Taylor & Francis Group.

EU4Digital. 2021. 2030 Digital Compass: the European way for the Digital Decade. Brussels: European Union.

Falkner, G., Heidebrecht, S., Obendiek, A. and Seidl, T. 2022. Digital Sovereignty - Rhetoric and Reality. Framework Paper for the Online Conference 28-29 April 2022. Vienna: Centre for European Integration Research, University of Vienna.

Foer, F. 2017. Facebook's war on free will. The Guardian.

Forbes. 2023. Top 100 Digital Companies. Forbes.

Forrester. 2022. Isabella, J. and Koetzle, L. (Hosts). Where Did Gaia-X Go Wrong? [Audio podcast episode]. Forrester.

Fraser, E. 2016. Data localisation and the balkanisation of the internet. SCRIPTed: A Journal of Law, Technology and Society.

GIZ. 2021. Citizen Engagement and Innovative Data Use for Africa's Development (DataCipation). Bonn: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH.

Global Privacy Assembly. 2022. 44th Closed Session of the Global Privacy Assembly: Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology. Global Privacy Assembly.

Government of India. e-Commerce Policy 2019. India Draft E-commerce Policy. New Delhi: Department for Promotion of Industry and Internal Trade.

Gravett, W. 2020. Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. African Human Rights Law Journal, 20(1), 125-146.

Hofmeyer, J., Wolf, N. and Cloete, D. 2022. SADC Futures of Digital Geopolitics: Towards African digital sovereignty. Occasional Paper 337. Johannesburg: South African Institute of International Affairs (SAIIA).

Hon, W.K., Millard, C., Reed, C., Singh, J., Walden, I. and Crowcroft, J. Policy, Legal and Regulatory Implications of a Europe-Only Cloud. Queen Mary School of Law Legal Studies Research Paper 191/2015, International Journal of Law and Information Technology.

HRW. 2022. India: Data Protection Bill Fosters State Surveillance. Draft Law Fails to Protect Privacy, Rights of Children. New York: Human Rights Watch.

Husami, K. 2022. China Splinternet, Is it a State-Controlled Alternative Cyberspace? London: Inside Telecom.

Internet Society. 2022. Navigating Digital Sovereignty and Its Impact on the Internet. Internet Society.

Iyer, N., Achieng, G., Borokini, F. and Ludger, U. 2021. Automated imperialism, expansionist dreams: Exploring digital extractivism in Africa. Pollicy.

Jili, B. 2022. The Rise of Chinese Surveillance Technology in Africa (part 5 of 6): Personal Data Vulnerabilities in Africa. Washington DC: Electronic Privacy Information Center (EPIC.org)

Jurcys, P. 2020. Personal Data Ownership. In: Towards Data Science. Medium.

Karkare, P. 2023. Unpacking digital sovereignty through industrial policy. Chapter in: Global approaches to digital sovereignty: Competing definitions and contrasting policy approaches. Maastricht: ECDPM.

Kokas, A. 2022. Trafficking Data. How China Is Winning the Battle for Digital Sovereignty. Oxford University Press.

Kugler, K. 2021. The Impact of Data Localisation Laws on Trade in Africa. Policy Brief 8. Johannesburg: Mandela Institute, School of Law, University of The Witwatersrand.

Kuner, C. 2014. Data nationalism and its discontents. Emory Law Journal Online.

Laidler, J. 2019. High tech is watching you. The Harvard Gazette.

Levin, Q. 2021. Review of the book *The Brussels Effect*, by Anu Bradford. Georgetown Journal of International Affairs 22(2), 307-310. Maryland: Project Muse.

Liu, L. 2021. The Rise of Data Politics: Digital China and the World. Studies in Comparative International Development 56, p.45–67. Springer.

López González, J., Casalini, F. and Porras, J. 2022. A Preliminary Mapping of Data Localisation Measures. OECD Trade Policy Papers, No. 262. Paris: OECD Publishing.

Lovells, H. 2023. Recent developments in African data protection laws - Outlook for 2023. London: Lexology.

Ma, A. 2018. China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you. Amsterdam: Business Insider Nederland.

Macaskill, E. and Dance, G. 2013. NSA files: Decoded. The Guardian.

Matambo, E. and Ugar, E.T. 2022. South Africa's Data Sovereignty Regulations: Merits and Possible Limitations. Policy Brief No. 2. Centre for Africa-China Studies, University of Johannesburg.

McKenna, M. 2016. Up in the cloud: Finding common ground in providing for law enforcement access to data held by cloud computing service providers. Vanderbilt Journal of Transnational Law.

Mishra, N. 2019. Building bridges: International trade law, internet governance, and the regulation of data flows. Vanderbilt Journal of Transnational Law.

NOYB. 2022. Statement on US Adequacy Decision by the European Commission. NOYB.

OJEU. 2018. Regulation (EU) 2018/1807 of the European Parliament and of The Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union. Brussels: Official Journal of the European Union. Brussels: Official Journal of the European Union.

OJEU. 2022. Regulation (EU) 2022/868 of the European Parliament and of The Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Brussels: Official Journal of the European Union.

Omino, M. and Rutenberg, I. 2021. Why the US-Kenya free trade agreement negotiations set a bad precedent for data policy. Global Partnership for Sustainable Development Data.

Paul, K. 2023. US moves forward plan to ban TikTok as AOC joins protests supporting app. The Guardian.

Ponciano, J. 2019. The Largest Technology Companies In 2019: Apple Reigns As Smartphones Slip And Cloud Services Thrive. Forbes.

Pottinger, M. and Feith, D. 2021. The Most Powerful Data Broker in the World Is Winning the War Against the US. New York City: New York Times.

Privacy in Africa. 2023. Bimonthly Update on Privacy in Africa (March and April, 2023). LinkedIn.

Rakesh, V. 2016. Aadhaar Act and its Non-compliance with Data Protection Law in India. Bangalore: Centre for Internet & Society.

Ray, T., Ajaykumar, S. and Patil, S. 2022. The Draft Digital Personal Data Protection Bill 2022: Recommendations to the Ministry of Electronics and Information Technology. Special report. New Delhi: Observer Research Foundation.

Razzano, G. 2021. Data Localisation in South Africa: Missteps in the Valuing of Data. Policy Brief 6. Johannesburg: Mandela Institute, School of Law, University of The Witwatersrand.

Republic of Rwanda. 2017. National Data Revolution Policy. Kigali: Republic of Rwanda Ministry of Youth and ICT.

Resha, G. 2021. Addressing the potential for African digital governance to facilitate inclusive development, rights, rules and revenues. 2021 Discussion Paper.

Rolf 2023. China's regulations on algorithms: Context, impact and comparisons with the EU. Friedrich Ebert Stiftung.

Svantesson, D. 2020. Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines. OECD Digital Economy Papers, No. 301. Paris: OECD Publishing.

Smart Africa. 2022. Smart Africa and NADPA signed an MOU to advance the enforcement and harmonization of personal data protection laws in Africa. Kigali: Smart Africa.

Tadesse Shiferaw, L. 2023. The EU-Africa partnership: One step forward, two steps backwards. ECDPM Commentary. Maastricht: ECDPM.

Tankard, C. 2016. What the GDPR means for businesses. Network Security Volume 2016, Issue 6,

2016, p. 5-8. ScienceDirect.

Teevan, C. and Domingo, E. 2022. The Global Gateway and the EU as a digital actor in Africa. ECDPM Discussion Paper 332. Maastricht: ECDPM.

Teevan, C. and Domingo, E. 2023. Integrating Digital Sovereignty in EU External Action. Chapter in: Global approaches to digital sovereignty: Competing definitions and contrasting policy approaches. Maastricht: ECDPM.

Thouvenin, F. and Tamò-Larrieux, A. 2021. Data Ownership and Data Access Rights: Meaningful Tools for Promoting the European Digital Single Market? In M. Burri (Ed.), Big Data and Global Trade Law (pp. 316-339). Cambridge: Cambridge University Press.

van der Berg, S. 2021. Data Protection in South Africa: The Potential Impact of Data Localisation on South Africa's Project of Sustainable Development. Policy Brief 2. Johannesburg: Mandela Institute, School of Law, University of The Witwatersrand.

van Lieshout, M. 2015. The Value of Personal Data. In: Camenisch, J., Fischer-Hübner, S., Hansen, M. (eds) Privacy and Identity Management for the Future Internet in the Age of Globalisation. Privacy and Identity 2014. IFIP Advances in Information and Communication Technology, Vol. 457. Cham: Springer.

Velluet, Q. and Beaubois-Jude, A. 2021. Africa: Why data centres are crucial for the continent's sovereignty. Paris: The Africa Report.

Vismay, G.R.N. 2019. Aadhaar and Data Protection: Compatible or Conflicting? The National University of Advanced Legal Studies (NUALS). Nagpur: Pen Acclaims.

Voight, P. and vom dem Bussche, A. 2017. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing.

Wood, S., Hoffmann, S., McFadden, M., Kaur, A., Wongsaroj, S., Schoentgen, A., Forsyth, G. and Wilkinson, L. 2020. Digital Sovereignty: the overlap and conflict between states, enterprises and citizens. Oxford Information Labs (OXIL). Plum Consulting.

World Bank. 2021. Ownership: Who owns personal data? Washington DC: The World Bank.

Wu, E. 2021. Sovereignty and Data Localization. The Cyber Project. Report. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs.

Yayboke, E., Ramos, C.G. and Sheppard, L.R. 2021. The Real National Security Concerns over Data Localization. Washington DC: Center for Strategic and International Studies (CSIS).

Zahn, M. 2023. No evidence of TikTok national security threat but reason for concern, experts say. New York: ABC News.