ecdpm The centre for Africa-Europe relations

DISCUSSION PAPER No. 344

Global approaches to digital sovereignty: Competing definitions and contrasting policy

By Melody Musoni, Poorva Karkare, Chloe Teevan and Ennatu Domingo

May 2023

There is little consensus on what digital sovereignty means. This results in different interpretations and policy implications. The different approaches to digital sovereignty have deepened geopolitical competition between the US, China and the EU.

In data governance, the US, home to leading big tech companies, prefers open data transfers. China strictly controls what data comes in and goes out of its territory while the EU‘s data protection laws put individual rights and privacy front and centre. We look at the impacts of the contrasting approaches of these major digital powers on developing countries as they seek a model of digital sovereignty that suits their political interests and development needs.

Major powers have taken similar lines in digital industrial policy, but there are significant differences in approaches and motivations. Defence and military spending was critical in propelling the US to its leading position in digital technologies by enabling investments in research and development into several critical digital innovations. China instead was motivated by the need to have domestic champions. The EU on the other hand focused on competition issues, slowly adopting industrial policies to create key European tech players. India carved a niche through its digital public infrastructure.

In this report, we look at these two interrelated policy areas, namely data governance policies and frameworks and industrial policies with ramifications for digital sovereignty. We assess the policy implications for the EU and provide recommendations to support effective cooperation and mutually beneficial partnerships with the Global South.

Table of Contents

List of Figures

Acknowledgements

The authors would like to thank the many policymakers and experts who shared their expertise with us throughout the research process, as well as external reviewers who commented on an earlier version. We would like to thank Annette Powell for her editorial assistance. This project was supported by the European Union.

All views are those of the authors alone and do not represent the views of ECDPM. The authors take responsibility for any factual errors. For any feedback or suggestions regarding future work, please contact cte@ecdpm.org, pk@ecdpm.org, mmu@ecdpm.org and edo@ecdpm.org.

Acronyms

AI	Artificial intelligence
APEC	Asia-Pacific Economic Cooperation
ATM	Automated teller machine
AU	African Union
AUC	African Union Commission
AWS	Amazon web services
BMZ	German Ministry for Development
CERT-in	Indian Computer Emergency Team
CHIPS	Creating Helpful Incentives to Produce Semiconductors and Science
CJEU	Court of Justice of the European Union
CLOUD	Clarifying Lawful Overseas Use of Data
DPG	Digital public goods
DPI	Digital public infrastructure
DSL	Digital subscriber line
DSM	Digital Single Market
DSR	Digital Silk Road
DTS	Digital Transformation Strategy
EAC	East African Community
ECOWAS	Economic Community of West African States
EEC	European Economic Community
EU	European Union
FDI	Foreign direct investment
FOSS	Free and open-source software
GAFAM	Google, Apple, Facebook (Meta), Amazon and Microsoft
GDIP	Green Deal Industrial Plan
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GIZ	Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
IBM	International Business Machines Corporation
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communication Technology
ID	Identification
IRA	Inflation Reduction Act
IT	Information technology
ITU	International Telecommunications Union
NADPA	Network of African Data Protection Authorities

NSA	National Security Agency
PIDA	Programme for Infrastructure Development in Africa
PIPL	Personal Information Protection Law
SADC	Southern Africa Development Community
SCA	Stored Communications Act
TTC	Trade and Technology Council
UN	United Nations
US	United States

Executive Summary

Digital sovereignty is a term widely being used by policymakers across the world. But there is little consensus about what it actually means, with cyber sovereignty, technological sovereignty and data sovereignty used interchangeably and yet having different connotations and significance for different actors. Overall, the debate on digital sovereignty cannot be divorced from the idea of sovereignty in international affairs.

Broadly speaking, digital sovereignty refers to the need for control over the physical layer (infrastructure, technology), the code layer (standards, rules and design) and the data layer (ownership, flows and use). It may be motivated by different interests such as protecting individuals (data protection), increasing the competitiveness of domestic firms (local content requirements or other industrial policy considerations), and protecting core democratic values or strategic public interests (maintaining sovereignty in critical infrastructure, national security), with major differences in how countries pursue these objectives.

The competition over approaches to digital sovereignty is playing out at multiple levels - in domestic industrial and governance strategies, in foreign policy and external infrastructure strategies, and at multilateral institutions, with major powers, namely the United States of America (US), China and the European Union (EU), promoting competing visions. Competition over technological innovation and development, backed by industrial policies, has deepened the geopolitical fault line between the US and China, and more recently fuelled a subsidy race between the US and the EU. Digital governance, and particularly data governance, has increasingly become an area of contention, coupled with a growing focus on *who* provides the basic infrastructure of the digital economy. These dynamics have spillover consequences for the rest of the world.

While the US's vision of a borderless cyber world where information flows freely without state interference is viewed with increasing unease even by its closest allies, China's conception and promotion of its vision of cyber sovereignty is also seen as controversial and enhancing state surveillance. As a third way between the US's 'surveillance capitalism', where largely unregulated firms harvest data to monetise it through targeted advertising to influence behaviours, and China's 'surveillance state', which uses technology like facial recognition, social credit systems, and censors the internet to monitor and surveil its citizens' activities, the EU had a more regulatory approach which puts individual rights front and centre in its conception of digital sovereignty. Its two-prong approach to digital sovereignty, which has accelerated since the beginning of the von der Leyen Commission in 2019 seeks to increase the robustness of the EU's regulatory toolkit and leverage the 'Brussels Effect' to shape global standards and the regulatory environment, while gradually embracing an active digital industrial policy to stimulate the development of European digital champions.

Developing countries want to develop their own approach to digital sovereignty based on their development needs and interests without having to choose between the US or China. Geopolitical competition and related tensions however are reducing the policy space for countries to do this. Some emerging powers, such as India, have developed relatively sophisticated visions of their own, while many countries in the Global South are still struggling to position themselves and develop a coherent approach to digital sovereignty. Nevertheless, discussions are growing, with African and Latin American theorists and activists also raising the risks of digital colonialism or data colonialism, and advocating for ways to achieve their own digital sovereignty.

India's approach to digital sovereignty aims to find a balance between national security, economic growth and development, and privacy concerns by, among other things, unrolling the digital public infrastructure 'India Stack'. African countries have also begun to emphasise their digital sovereignty through a variety of different measures. At the continental level, the Digital Transformation Strategy reflects an emerging interest in digital sovereignty, although it does not develop on what this concept means for Africa in any great detail. The African Union's (AU)

Data Policy Framework begins to provide a more comprehensive vision on data governance that supports innovation and the better provision of public and private services.

Countries' approaches to the governance of personal and non-personal data are seen as an extension of their sovereignty, and an essential part of their approach to digital sovereignty. Governments approach it in different ways given their unique social, economic and political environment, technological capabilities, domestic priorities and digital foreign policy, indicating that there is no 'one size fits all'. Other factors such as increasing (digital) geopolitical tensions, risks of foreign government surveillance, and concerns of digital colonialism also impact national data governance frameworks.

The regulation of personal data and non-personal data is also handled quite differently from one government to the other. Governments usually develop data protection laws to protect their citizens' personal data in line with clearly defined principles with safeguards to prevent the abuse, including by big tech. The EU's General Data Protection Regulation (GDPR) is a comprehensive law protecting personal data and widely seen as an international best practice, with the EU seeking to influence international standards and norms with the GDPR. The EU is also leading the way by developing new legal frameworks such as the Data Act and Data Governance Act which regulate the sharing, processing and innovative use of non-personal data while facilitating data sharing among trusted actors, strengthening mechanisms to increase data availability and overcoming obstacles to the reuse of data. For the EU, an important aspect of digital sovereignty is about leading in norms and standards setting, while advancing the protection of fundamental rights and values.

The US and China have contrasting approaches. While most big tech companies are from the US, the country does not have a data protection law at the federal level and instead, some states have promulgated their own data protection laws. Not only is it unclear to external players how personal data is treated once it is transferred into the US, transfer of personal data outside the US also does not have restrictions in line with the ethos of free and open data flows, which makes it easier for US firms to do business at a global level. More broadly, the US reliance on corporate self-regulation and support for multi-stakeholder initiatives that gave US firms an outsized role, has been viewed with suspicion by China, where the state has played a more prominent role. In line with the growing trend on data protection, China recently adopted a data protection law, though it still leaves room for the government to exercise surveillance. Further, Chinese laws place strict restrictions on cross border data flows, with mandatory requirements for local storage of data, which may conflict with laws from other countries as shown by the 2021 Data Security Law which does not allow foreign law enforcement authorities to access data stored in China unless the Chinese authorities have approved whereas the Clarifying Lawful Overseas Use of Data (CLOUD) Act authorises US authorities to demand access to data held by US companies overseas regardless of where it is located.

Developing countries have also been making some progress in defining their data governance approaches. India is in the process of developing its own data protection law, which is modelled along the GDPR principles as well as Singapore's data protection law, but allows greater exceptions to access data for security purposes than the GDPR. This is timely considering the amount of personal data processed under its Aadhaar digital ID system. African countries are also developing their own data protection laws, with some leaving more room than others to exercise discretion in processing data, along with sometimes unclearly defined national security exceptions. The African Union's Convention on Cyber Security and Personal Data Protection can potentially create the basis for a unified continental approach to data protection once it comes into operation. The AU's Data Policy Framework seeks 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.

Governments are investing in local data centres as there is a growing perception that whoever controls the physical infrastructure exercises sovereignty over data, with fears that foreign control on such infrastructures would invite foreign surveillance. National security interests and economic benefits have motivated the adoption of data localisation measures but countries also have competing approaches to data localisation. The US approach is opposed to data localisation and advocates for free flow of data. China, on the other hand, exercises a strong version of digital sovereignty with strict data localisation rules as well as stringent security assessments for cross-border transfer of data. The EU, driven by its human-centric approach to data, allows for conditional transfer of data with requirements of data protection principles and safeguards in line with the GDPR. India and Africa have a hybrid approach which seeks to promote local storage of data while permitting data transfers against defined rules.

Though there are differences in data governance frameworks which are shaped by broader visions of digital sovereignty, cooperation on, and development of, principles on data processing and data sharing is necessary because ultimately the value of data is generated not from local storage but from sharing and using it.

As digital sovereignty has come to encompass technological sovereignty or indigenisation to build and/or strengthen domestic technological and manufacturing capabilities, digital and industrial policies have also become closely intertwined. While for some, it may be about boosting the national industrial production through domestic champions, for others it may be about risk mitigation and securing the supply of inputs, with digital industrial policies having a strong element of geopolitical considerations.

Although the US, China and the EU approach digital sovereignty very differently, their digital industrial policies and instruments have similarities, with a prominent role played by the state combined with experimentation and substantial investments in research and innovation. The motivations for these policy actions were very different, however. For instance, defence and military spending played a critical role in propelling the US to its leading position in digital technologies by enabling investments in research and development into several critical digital innovations. China's digital industrial policies on the other hand were motivated by the need to have domestic rivals to foreign giants, by learning along with the private sector rather than being in the driver seat. Given the tensions of managing the role of the state, especially its subsidies in a confederation of states, the EU has instead focused on ensuring free and fair competition in the past decades, although more recently it has started to focus on developing European digital champions and lessening critical dependencies.

As its dominance is challenged by a rising China, there is a strong bipartisan support for industrial policy in the US with the Inflation Reduction Act (IRA) and the Creating Helpful Incentives to Produce Semiconductors and Science (CHIPS) Act. China on the other hand, with a changed approach from the 'hide your strength and bide your time' under Deng Xiaoping to greater assertiveness under Xi Jinping, has its Made in China 2025 policy complemented by Internet Plus, which is in turn reflected in its 14th five-year plan. The EU has several policy documents which reflect its ambitions to enhance its strategic autonomy and strengthen its technological leadership while leveraging its core regulatory competences. Its Digital Markets Act (DMA) seeks to tackle the network effects of large online platforms to ensure a fairer business environment, while the European Industrial Strategy aims to support the EU's twin digital and green transition and is complemented by a host of other regulations and policies.

Nevertheless, there are important differences in their approaches, with a significant element of competition. The race to build domestic manufacturing capabilities for semiconductors has become one of the major geopolitical fault lines between the US and China. Current US policies aim to support the domestic industry, but coercive sanctions also highlight the growth of a 'China-proofing' strategy in light of the current geopolitical tensions and tech war. In that sense, there are some similarities with the US-Japan rivalry in the 1980s when the US's hegemony was challenged. In contrast, to escape a potential 'middle-income trap', and counter its negative image of engaging in intellectual property theft, China has increasingly focused on building advanced domestic capabilities to transform itself from the assembly and manufacture of individual components into a production hub of high-tech products. The EU has a distinct regulatory approach that seeks to rein in the powers of platform giants, and as mentioned above, lead on setting global norms and standards, while also pushing for more investments into building their own digital capabilities.

The effects of digital technologies and digital industrial policies in the above established powers has significant implications for developing countries. Rather than technological leadership which seems the objective of digital industrial policies among the established powers, developing countries need policies suited for technological catch-up. In most cases, their development needs may not neatly fit in any of the models followed by the established powers, and in fact their economic and political relations straddle multiple blocs to meet their varied developmental needs. While countries are increasingly adopting digital policies and regulations to govern the flow of data to achieve broader objectives such as national security or personal data protection, their links to development objectives of conventional industrial policies, of creating and shaping markets to raise production and productivity, are unclear.

Although digital industrial policies in established powers are more about innovation and building digital hardware and software, in developing countries the focus should be to acquire key (digital) technologies to support strategic sectors like agriculture and manufacturing. This is because digital technologies can be deployed to enable efficiency gains in production - faster and customised production processes, optimisation and waste reduction, and improved product quality and safety. This is necessary in order to avoid a further widening in the productivity gap between these countries and the established powers. This can be sought through greater linkages to lead firms in global value chains (GVCs) for technology transfer and incremental learning, rather than by creating national rivals to global giants.

Lessons can be drawn from rising powers such as India which has sought to innovatively balance competing objectives and priorities. Spurring digital innovation by using free and open-source software (FOSS), India’s technological advances are embodied in its digital public infrastructure which provides government services through India Stack which is a comprehensive digital identity, payment, and data-management system. In contrast, the development of the digital economy in Africa will have to start by increasing access to the internet, with a focus on not just the consumption of digital technologies but also their productive use. From that perspective, the use of digital technologies to upgrade value chains has been limited in many African countries with structural challenges around infrastructure, finance, and a limited productive base. As mentioned above, navigating the current geopolitical tensions adds another layer of complexity and challenges for countries in seeking digital development for economic prosperity.

The European approach to digital sovereignty is increasingly evoked in EU foreign and security policy, as well as in the EU’s wider international partnerships, but the EU remains vague about defining this term when using it at multilateral fora or in its relations with other countries. The domestic usage is multifaceted and encompasses a wide range of regulatory measures, coupled with a growing focus on industrial policy. There is a strong focus on individual rights, while at the same time, a growing interest in supporting European businesses.

For more effective cooperation at the international level, working more closely with others in a collaborative and open-minded way. The EU would need to demonstrate how its policies back up its promise of supporting digital sovereignty in partner countries, and developing more respectful and mutually beneficial partnerships. At present, with intense geopolitical competition around investments and international partnerships with developing countries in the Global South, if the EU is seen to be ‘preaching’ and trying to externalise its vision and regulations, this may ultimately be counterproductive and give rise to accusations of neocolonial practices. This means that the EU should work with others to come up with a shared basic understanding of this term.

In order to begin to do this, the EU should demonstrate consistency between the concept of digital sovereignty in its internal and external policies in line with the aims of the so-called "Geopolitical Commission." As it focuses more and more on industrial policy to respond to the geopolitical environment in which it operates, the EU should also integrate partner countries' interests and ambitions with regard to industrialisation in its engagement with them, supporting local technology hubs and funding research and innovation partnerships. It will also need to show an openness to compromising with, and learn from, partners across the world to come up with common approaches to key concepts that are central to the European approach to digital sovereignty, including developing an inclusive approach to "human-centric" digital transformation. Further, the EU will need to demonstrate how its approach to data governance and to digital governance more broadly can be meaningful to others given the vastly different development contexts and political interests.

Developing shared approaches to digital sovereignty - both with traditional partners, such as the other G7 members, as well as with emerging powers like India, and regional blocs such as the African Union, will be essential to the EU's geopolitical aims regarding digital governance. Such cooperation, which entails cross-learning rather than a simple externalisation of EU regulations, can help avoid accusations that EU actors preach to partner countries in the Global South. Such an approach is beginning to emerge vis-a-vis certain partners, and could be extended to wider partnerships with the Global South.

We look at EU-US collaboration in the Global South, and at relations with India and Africa - notably the African Union - in order to illustrate different kinds of partnerships with different kinds of actors. For instance, despite many differences, the EU and US largely enjoy a relationship of mutual respect, finding common cause where they do have clear shared interests, including increasingly in the desire to support investments in the Global South. Over the past years, the EU and India too have been strengthening their bilateral relationship, driven by the changing geopolitical environment and India's growing ambition to balance competition over critical technology supply chains and a reduced reliance on China. Despite its autonomy and arguably differentiated approach compared to the EU's GDPR, India stands to be a strong partner for the EU when seen through a holistic rather than a solely normative lens. The EU partnership with the African Union and key African states on digital transformation is very new and should entail a real negotiation around what digital sovereignty means for policymakers on each side and how this can actually be implemented in practice.

Setting the scene

Digital sovereignty, and the related concepts of cyber sovereignty, technological sovereignty and data sovereignty are being employed more and more widely by policymakers across the world. There is little consensus about what these terms actually mean, and indeed for different global actors, it often has very different connotations and policy consequences.

Broadly speaking, digital sovereignty refers to the need for control over the physical layer (infrastructure, technology), the code layer (standards, rules and design) and the data layer (ownership, flows and use). It may be motivated by different interests such as protecting individuals (data protection), increasing the competitiveness of domestic firms (local content requirements or other industrial policy considerations), and protecting core democratic values or strategic public interests (maintaining sovereignty in critical infrastructure, national security).

However, while global actors appear to be broadly on the same page in terms of the perceived need to stimulate homegrown industries, notably in high-tech areas with potentially significant national security consequences, there are major variations in how these actors approach the governance of these technologies, and particularly in their approaches to data governance.

Competition over technological innovation and development, backed by industrial policies, has become the major geopolitical fault line between the United States (US) and China today, while it is also fuelling a subsidy race between the US and the European Union (EU). These domestic efforts to incentivise cutting-edge technologies and to become self-sufficient in vital components of the digital economy - notably chips - will undoubtedly have spillover consequences for the rest of the world.

Digital governance, and particularly data governance, has increasingly become an area of contention, with a growing focus on *who* provides the basic infrastructure of the digital economy, including in third countries across the world. Fearing data colonialism, where data is extracted by foreign firms from marginalised communities without their knowledge or consent for profit and to feed their own technological development, a growing number of countries are grasping for ways to protect citizens' data and ensure national security. Other motivations such as spurring local innovation for economic development have also made data governance a key policy issue. Yet, approaches vary greatly - both amongst the global powers and in the Global South - from no controls to strict data localisation.

The competition over approaches to digital technologies and digital sovereignty is playing out at multiple levels. In domestic industrial and governance strategies, in foreign policy and external infrastructure strategies and at multilateral institutions, major powers have been actively promoting competing visions - they have been vying for positions in top jobs down to very technical working groups. Some emerging powers, such as India, have developed relatively sophisticated visions of their own, while many countries in the Global South are still struggling to position themselves and develop a coherent approach to digital sovereignty.

This work will examine: (i) why digital sovereignty has emerged as such a geopolitically charged term, (ii) how the different approaches of different global and emerging powers are playing out, and (iii) the implications for EU policy and digital partnership with developing countries in the Global South, including in Africa, Latin America and the Caribbean (LAC), and Asia-Pacific. It will delve into two interrelated areas of policy with major ramifications for digital sovereignty - data governance (chapter 1) and industrial policy (chapter 2). It argues that a realistic assessment of the international implications of both will be necessary to offer an attractive and meaningful view of digital sovereignty in international affairs. Finally, it will propose a series of policy recommendations for policymakers in the EU in engaging with counterparts in the Global South (chapter 3).

Origins of the debate

The debate about digital sovereignty cannot be divorced from wider debates about sovereignty in international affairs. The question of sovereignty is itself a complicated one, and one that has long been a central bone of contention in international affairs. For China, and many postcolonial countries, protecting full state sovereignty continues to be a core tenet of their position in international affairs, and China has sought to use the United Nations (UN) system to defend its vision of sovereignty. The interventionism engaged in by the US and some allies in the 1990s and 2000s in the name of liberal internationalism, most notably with the invasion of Iraq in 2003, was thus anathema to many countries across the world. The question of sovereignty is, of course, also central to current debates about the Russian invasion of Ukraine, raising this question to the forefront of international affairs once again.

In the area of digital technologies and internet governance, the liberal internationalism of the US was taken even further, promoting a cyber world without borders, where information would flow freely across the world with no state interference. This vision was always viewed with suspicion by states such as China for which state sovereignty should also apply to the online world, but in more recent years, this ideal of a completely open and unregulated internet has come to be viewed with unease even by the US's closest allies in Europe, Japan and elsewhere. Edward Snowden's revelations on the US government's practices under the US Cloud Act and growing concerns about 'surveillance capitalism,' where (US) firms harvest data to monetise it through targeted advertising to influence behaviours have added to the concerns. This has led to a growing focus on regulating the online space and developing indigenous technologies across the world, albeit with varying approaches from different established and emerging powers.

China introduced the concept of 'cyber sovereignty' (wangluo zhuquan 网络主权) and with its Great Firewall sought to preserve a strong idea of state sovereignty: "With territorialisation, Beijing seeks to delineate its national boundaries in cyberspace, ensure that online processes affecting important Chinese interests take place within those boundaries, and unwanted activities can be barred from entering" (Creemers 2020: p.10). At the same time, the blocking of major US companies allowed for the emergence of local champions, providing more or less identical services in a process of 'indigenisation' (Ibid.).

Over time, this largely domestic process was coupled with a growing externalisation process as China sought to develop markets for its technology abroad, by developing the Digital Silk Road. At the same time, China and Russia increasingly adopted a more proactive cyber diplomacy at international institutions that was intimately connected with their domestic visions regarding cyber sovereignty and state control. China developed sophisticated cyber diplomacy at institutions such as the International Telecommunication Union (ITU) that allowed it to defend its vision and interests on the international stage. This included China's promotion of the controversial New IP (internet protocol) proposal at multilateral fora, which would have created a new internet based on new standards and protocols with a view to responding to potential future challenges with the existing architecture. However, the proposals were viewed by critics as a way of putting greater control of the internet architecture in the hands of states, thereby enhancing potential state surveillance. Critics from the EU and elsewhere also consider it not to be sufficiently developed in terms of the technical specifications, and to not include sufficient consideration around interoperability with the existing internet (Murgia and Gross 2020; Degezelle et al. 2022). While the original proposal was rejected, China continues to promote New IP via other channels. Russia also tabled resolutions on cyber sovereignty at the UN General Assembly that managed to garner substantial support across many parts of the Global South.

Although the EU had already adopted the General Data Protection Regulation (GDPR) in 2016, it was the election of Emmanuel Macron in France in 2017, and the subsequent agenda of the von der Leyen Commission, appointed in late 2019, that really began to bring the debate around digital sovereignty into the mainstream policy debate in Europe. Although the focus of different actors in Europe tends to vary, the European approach broadly encompasses a strengthening of its digital governance model, coupled with a growing focus on developing home-grown European technologies. On the governance front, the EU is seeking to build on GDPR to develop an approach that puts European citizens' individual rights front and centre of its conception of sovereignty, and at the same time, it seeks to build on existing antitrust laws to improve competition and create greater space for innovation. This has gradually been accompanied by a growing focus on industrial policy, although there are still many debates around the appropriate role for states and the EU in driving forward industrial strategy.

India, like other developing countries, does not want to choose between the US and the Chinese digital sovereignty models and is developing its own approach based on its own interests and development context. India's approach to digital sovereignty, supported by Digital India and Make in India, aims to find a balance between national security, economic growth and development, and privacy concerns. Yet, this approach is also quite distinct from the EU's approach, allowing a much stronger role for the state and less strenuous standards of data protection. It aims to boost the growth of its domestic tech industry, which includes the unrolling of the digital public infrastructure India Stack, to respond to growing Chinese influence on its market and (cyber)security threats in the region. These have been driving forces of its digital sovereignty approach, and in turn of its digital diplomacy (Basu 2021). For example, the Indian Digital Personal Data Protection bill draws principles on data regulation from both the EU's GDPR and Singapore's data protection law and has been considered by some African countries as a model that would respond to some of the challenges they encounter when trying to adopt a GDPR inspired data protection policies, especially the issues related to data adequacy (see Musoni 2023 in this report for more). However, India still needs to strike a balance between security and economic interests given its reliance on foreign, especially Chinese, firms for its infrastructure (Burrows and Mueller-Kaler 2021). India has been strengthening its role in debates on digital governance at multilateral forums despite being criticised for being ambiguous when it comes to its selective alignment. The Digital India Act, which will govern all digital aspects, and its data protection bill, both in review, will be key policy tools that will strengthen the country's digital sovereignty and make it a key partner, including with the EU, on setting standards around regulating artificial intelligence (AI) and machine learning (ML) technologies (Chin 2023).

Discussions about digital sovereignty are growing across other parts of the world also. African and Latin American theorists and activists have increasingly raised the risks of digital colonialism or data colonialism, and begun to advocate for ways that their countries or regions might take steps towards achieving their own digital sovereignty. This has notably included the drafting of a letter to then-presidential candidate Luiz Inácio Lula da Silva by activists and researchers in Brazil in August 2022, entitled 'Emergency Program for Digital Sovereignty,' denouncing the data extractivism at the heart of contemporary digital development, and calling for the country to address its dependencies (Bosoer 2022). Japan, South Korea and Taiwan have each made themselves indispensable nodes in global value chains (Pons 2023).

A number of African countries have also begun to emphasise their digital sovereignty through a variety of different measures. At the continental level, the Digital Transformation Strategy gave some initial hints of an emerging interest in digital sovereignty but did not develop this concept in any meaningful way. The African Union (AU) Data Policy Framework begins to provide a more comprehensive vision on the side of data governance and its potential to feed emerging digital and industrial sectors. Yet, at present, the approach tends to be somewhat fragmented with different African countries adopting very different approaches to questions such as data localisation and digital taxation. It will now be essential to step up the actual implementation of the Data Policy Framework in order for African countries to work together towards achieving a shared vision for data governance as part of a wider pursuit of digital sovereignty.

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.

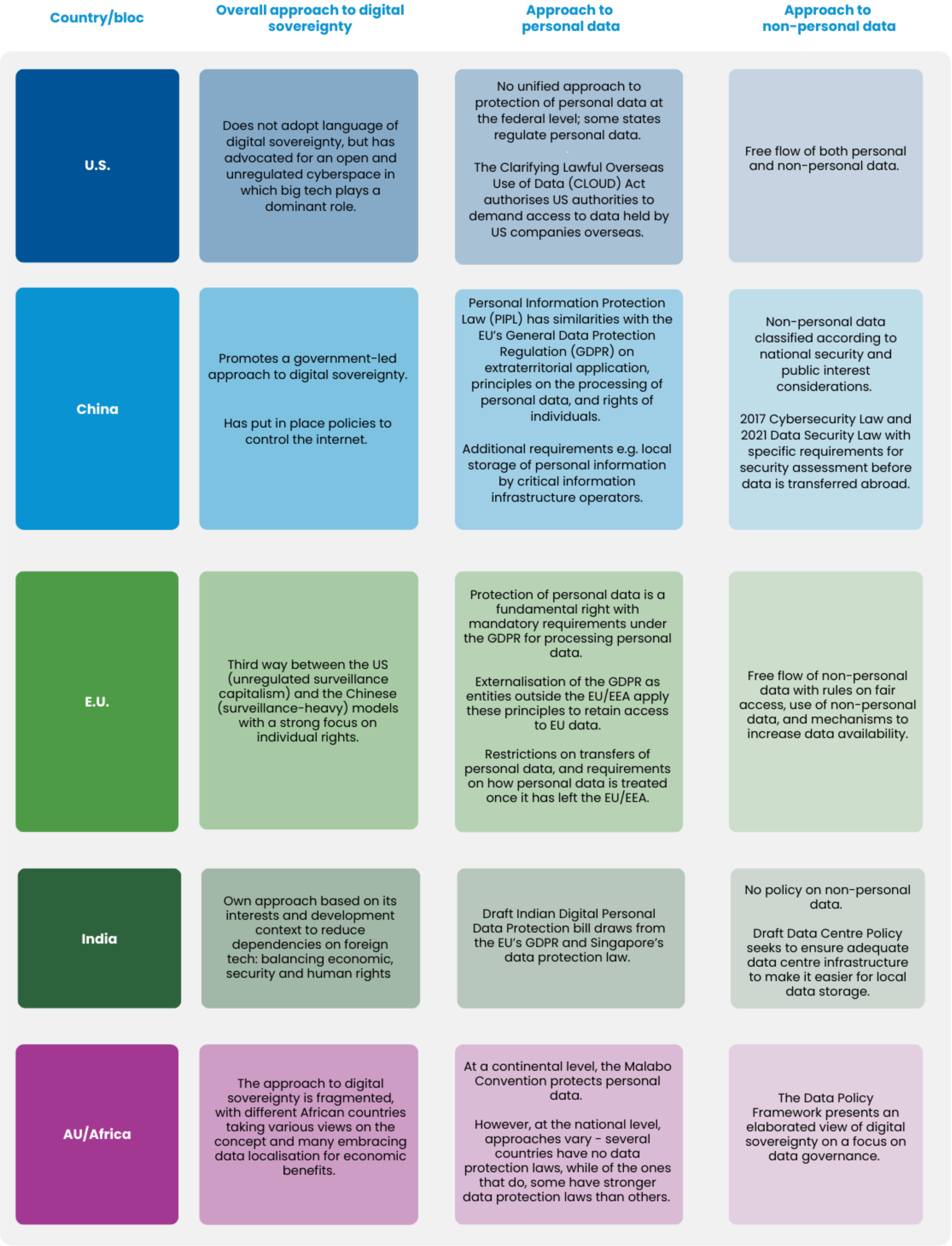
Africa

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.

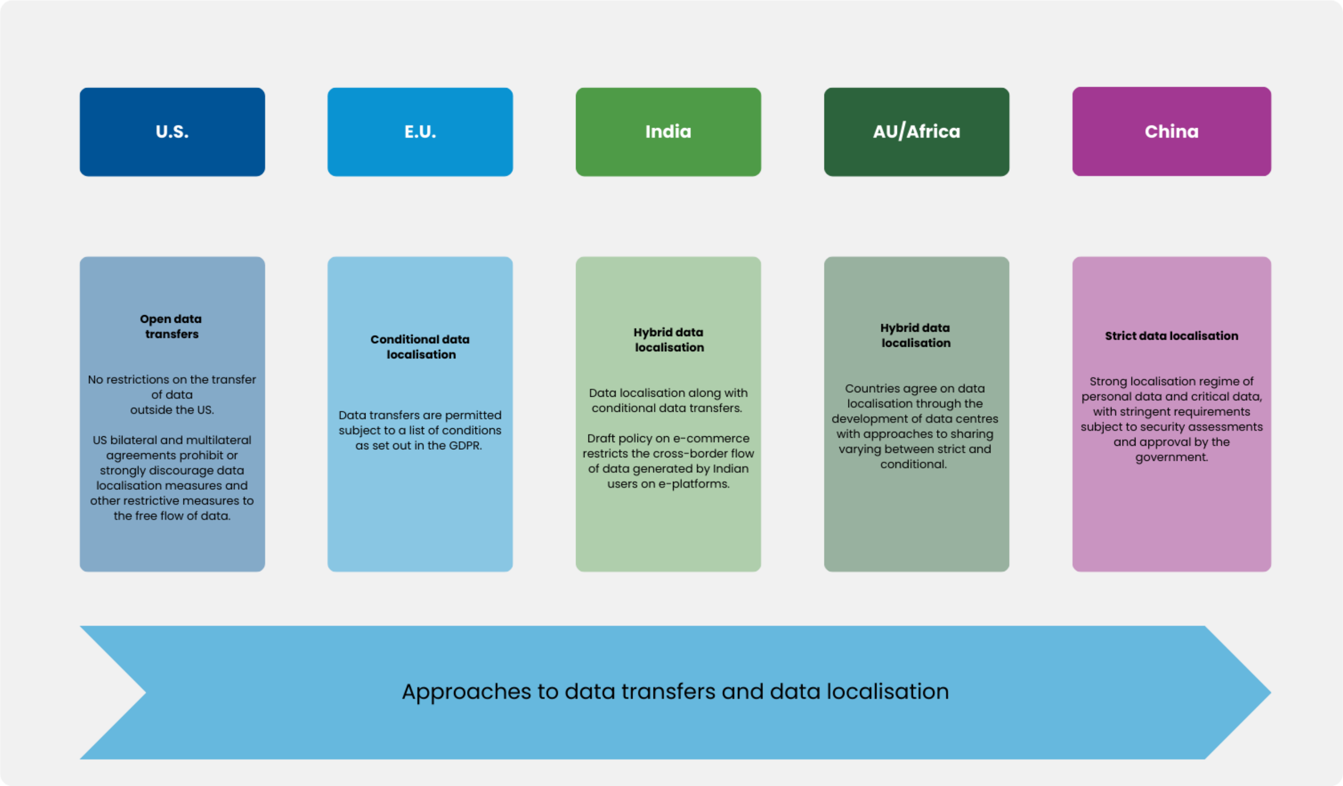
[3] Nigeria's Guidelines for Content Development in ICTs.

[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.

Chapter 2 – Unpacking digital sovereignty through industrial policy by Poorva Karkare

1. Introduction

Digital and industrial policies are closely intertwined, with governments increasingly seeking to support industrial development with digital policies or to channel digital policies towards specific objectives. As highlighted in the introduction to this series, the term digital sovereignty has different policy implications for different actors ranging from governance issues to rein in the excesses of tech giants (see Musoni 2023 in this report), to the imperative to create national champions or to the need to remain a relevant geopolitical player. As a result, digital sovereignty increasingly encompasses indigenisation or technological sovereignty with ambitions to build and strengthen national capabilities in digital infrastructure, including networks and cloud services. Established digital powers - the United States of America (US), China and the European Union (EU) - also compete to lead the global digital transformation and promote their own model of digital governance, which is reflected in their industrial policy design, with a profound impact on other countries. This note discusses the digital industrial policies of the major powers and draws implications for the prospects and development trajectories of low and middle-income countries.

Governments have become increasingly aware of the need to boost production by securing input supplies and investing in the development of domestic manufacturing capabilities to produce semiconductors as well as innovate in, and harness digital technologies such as artificial intelligence (AI), and quantum computing for local industrial development. Risk mitigation considerations further strengthen the case for digital industrial policies - governments are wary of their dependence on a few countries, especially China, given the risk of supply chain failures as experienced during the COVID-19 pandemic, or due to the current geopolitical tensions.

Digital industrial policies vary across countries, using the power and influence of the state as: a *facilitator*, through joint ventures and attracting foreign direct investment (FDI); *regulator* by setting rules around the use and flows of data); *producer* through state-owned enterprises; and a *buyer* through procurement. Digital industrial policies are enabling countries to adapt to the changing geopolitical environment and in some cases reflect the need to come out ahead in the technological race.

While the United States of America (US), China and the European Union (EU) - as established digital powers - are following distinct pathways to digital sovereignty and industrial policy, emerging powers like India show another course for developing domestic capabilities in a context-specific way. As the US and the EU do not enjoy the cultural, economic and technological hegemony they did in the past, and non-Western alternatives, in all their heterogeneity, have emerged to show different ways of organising societies, it is important to understand these different models and related policies.

This chapter seeks to explore the different models for promoting digital industrial policies. Section 2 compares the different approaches among established powers to digital industrial policies. While the context and motivation of their industrial policies are very different, the policies deployed are not very dissimilar. With competition among these models to assume digital leadership, the current geopolitical environment exacerbates the challenges to digital transition in developing countries. Section 3 discusses the case of India as a rising power balancing competing domestic priorities and navigating global geopolitical currents, and also argues that development needs in Africa will require yet another approach to enable its integration into the global economy. Section 4 concludes with some implications. Further recommendations for the EU can be found in Chapter 4 of this report (See Teevan and Domingo 2023).

2. Established digital powers

Although the US, China and the EU approach digital sovereignty very differently, their digital industrial policies and instruments are similar. There is a prominent role played by the state, combined with experimentation and substantial investments in research and innovation. While these policies have been introduced in incomparable contexts, geopolitical competition has shaped the policy choices of these established digital powers, with elements of coercion, retaliation and regulation to affirm their influence. Their foreign policy and international partnerships in turn reflect these realities - reflecting a two-way relationship between geopolitics and digital industrial policies.

The **US** has long been at the forefront of digital technologies. It has maintained its hegemony through industrial policy aimed at developing critical technologies, especially when faced with potential competitors, such as Japan in the 1980s. More recently, industrial policy has made a strong comeback in the US with the Inflation Reduction Act (IRA) and the Creating Helpful Incentives to Produce Semiconductors and Science (CHIPS) Act. Pushing the rhetoric of a “free and open internet” on the global stage, the American tech industry has largely relied on corporate self-regulation in their harvesting and use of data. The government-supported multi-stakeholder approach to global internet governance through organisations like the Internet Corporation for Assigned Names and Numbers (ICANN) has given its tech giants an outsized role in global standard setting for a long time (eds. Kokas 2022), an approach that continues to this day. Despite rising political polarisation, the US has largely embraced a bipartisan approach to industrial policy in response to the rise of China.

As a military and economic power, **China**’s influence has grown to shape global norms, standards and rules around the internet and global digital infrastructure with an emphasis on the role of the state. This contrasts with the multi-stakeholder approach through the ICANN which is perceived as being largely aligned with US interests. Through its Digital Silk Road (DSR), part of the broader Belt and Road Initiative (BRI), China has built critical digital infrastructure in multiple developing countries to gain market share for domestic tech players, especially in Africa. These initiatives are seen with scepticism and concern by traditional superpowers (the US and the EU) as Chinese attempts to promote technology-enabled authoritarianism, or techno-authoritarianism, going against personal freedoms and national sovereignty (Domingo and Tadesse Shiferaw 2022a). China-US geopolitical competition is often framed as a zero-sum game where the US perceives China to be a security threat while the latter seeks to challenge the former’s dominance in the international system and perceives Western opposition as an attempt to thwart its development (Thibaut 2022).

For decades, the **EU** and its predecessor, the European Economic Community (EEC), rejected industrial policy in favour of a regulatory approach that favoured competition policy above all else. At the core of the EU Single Market was the idea of creating a level-playing field amongst member states through the creation of regulations and standards, and enforcement of competition law. The belief was that this approach would stimulate innovation, while the EU hoped to export its model via bilateral and multilateral trade agreements (De Ville 2023) and through the so-called ‘Brussels effect’, where EU standards become de facto global standards (Bradford 2020). This however is changing with the bloc actively embracing digital industrial policies to complement its regulatory approach under a two-pronged strategy.[9]

While all three powers are therefore using industrial policy to pursue their own vision of digital sovereignty, with an element of competition among these models to achieve digital leadership, it is important to understand the implications and the effect on **developing countries** whose needs may not neatly fit in any of the models. There is a rise in digital policies in these countries to govern the flow of information in line with broader objectives such as

[9] This approach with the aim of becoming a geopolitical player in the digital economy has accelerated since the beginning of the von der Leyen Commission in 2019.

national security or personal data protection (see Musoni 2023), however their links to development objectives of conventional industrial policies such as technological catch-up are unclear. Digital technologies can be deployed to enable efficiency gains in production - faster and customised production processes, optimisation and waste reduction, and improved product quality and safety. However, their use remains concentrated in a few, mainly advanced countries (Lema and Rabellotti 2023). There is a need to facilitate technological and economic catch up, through integration into global value chains, for the Fourth Industrial Revolution (4IR) (Foster and Azmeh 2019).[10] Digital industrial policies should therefore aim to push domestic firms to acquire key (digital) technologies in strategic sectors to support domestic industries such as agriculture and manufacturing. Given the relative lack of skills as well as limited economies of scale, linkages to lead firms in global value chains (GVCs) can provide opportunities for technology transfer and incremental learning (Ibid.).

2.1. Comparing digital strategies - different motivations, similar tools

The US

The US is the supreme tech empire globally (Kwet 2021; Mirrlees 2020),[11] with a size, reach, profits, and power that is far greater than any other country, including China. Eight of the top ten global big tech firms are American[12] and only one is Chinese (Tencent Holdings). Silicon Valley is home to 12 of the 20 most visited websites, compared to two in China.[13]

While the US has been a beacon of private sector innovation, in many ways the central role played by the state has been underestimated. Long-run strategic (rather than short-term venture capital) investments and mission-oriented public policies were instituted to 'create' and 'shape' markets, rather than just 'fix' market failures as the role of the state is often relegated to (eds. Mazzucato 2013).[14]

Specifically, defence and military spending played an essential role in developing the US semiconductor industry and enabled private firms to innovate cutting-edge technologies throughout the Cold War and beyond.[15] This spending gave many private sector actors their first major contracts that allowed them to invest in the necessary R&D (especially commercialisation of previous scientific research), improve their technologies over time, and scale up production (Ibid; eds. Miller 2022). The imperative to maintain military and technological supremacy distinguishes the development of the US digital industry from others like the EU which did not have these ambitions and hence lacked the scale of investments seen in the US. The rise of another dominant player challenges the US's superiority

[10] Technologies under Industry 4.0 (or Fourth Industrial Revolution - 4IR) include 1) Smart Manufacturing and Service Technologies for automation and decentralisation of tasks and including advanced robotics, 3D printing, Internet of Things (IoT) and 2) Data Processing Technologies for interconnection and data exchange including big data blockchain, cloud computing, machine learning and AI (Lema and Rabellotti 2023).

[11] The country leads in search engines (Google), smartphone/tablet and desktop/laptop operating systems (Google Android, Apple iOS, Microsoft Windows, MacOS), email (Gmail, Outlook, Yahoo) cloud infrastructure and services (Amazon, Microsoft, Google, IBM), social and business networking platforms (Facebook, Instagram, Twitter, LinkedIn), entertainment (YouTube, Netflix, Hulu), discussion forums and encyclopaedia (Reddit, Wikipedia, Quora), transportation (Uber, Lyft), online advertising (Facebook), among other things.

[12] Apple, Microsoft, Alphabet-Google, Intel, IBM, Facebook, Cisco Systems, and Oracle.

[13] See https://www.similarweb.com/top-websites/ Though increasingly Chinese apps are becoming popular too - four out of five most popular apps in the US are Chinese (Lu et al. 2023).

[14] Taking the example of an iPhone the author argues that the state was behind every big innovation - the internet, cellular communication, GPS, microchips, Siri, touchscreen.

[15] Even as around 90% of the chips today are used for civilian purposes, characterised by high demand but low prices, it is the defence spending, which paid top dollar but remains a small consumer, that drove these innovations in semiconductor technologies to originally power the US military (eds. Miller 2022).

in this domain and may go some way in explaining the current rivalry with China, just as it did with Japan in the 1980s.[16]

Apart from its dominance in digital hardware and software innovations, the US is also home to the largest firms that today have come to become the face of the platform economy. Aiming to facilitate exchanges between consumers and producers, the platform economy has disrupted existing business models in a range of sectors, especially reducing the need for intermediaries, while in others it has been complementary to offline activities. At the same time, this has raised issues of data extractivism.

These firms have been at the forefront of harvesting user data to predict consumer patterns and monetise the data through targeted advertising to influence behaviour, also coined 'surveillance capitalism' (Laidler 2019). The government also leverages big tech's model of surveillance capitalism to produce data profiles and monitor global populations for predictive analytics of potential threats to the US (Mirrlees 2020). With operations spread across the world, these firms have achieved near-monopolistic positions and stifled competition through anticompetitive behaviour, with regulations across the world largely trailing the developments in this sector. Thus, overall, commercial considerations that drive companies have worked in a symbiotic way with the strategic considerations that drive the nation.

China

China's industrial policy emerged from the need to build domestic production competencies, further propelled by the perceived (existential) threat from the US while strengthening the legal competencies to regulate big tech and enforce rules. The beginning of these ambitions predate current geopolitical competition and are already evident in the Great Firewall in 1997, soon after China's introduction to the internet in 1994, which aims to not only control the flows of data but also "foster domestic rivals to foreign giants" (Creemers 2020).

Given that the skills base was mostly in the private sector, the government engaged in strategic public-private partnerships. This pragmatic approach is reflected in early partnerships with foreign players like Cisco, Samsung, Sony, and Bosch (Huang and Tsai 2022) before these were phased out as domestic capabilities were built. Along with FDI in joint ventures and technology transfer, firms also depended on government contracts (Ibid.). These paved the way for future domestic big tech firms such as Huawei, Hytera, ZTE for hardware and telecom equipment; with Baidu, Tencent, and Alibaba being the internet giants. The adoption and enforcement of national standards with limited influence of foreign businesses also ensured that domestic firms were preferred in government procurement processes (Ibid.; Liu 2021). As a result of these and other enabling policies, China's digital sector transformed from mostly importing to almost exclusively domestic (Huang and Tsai 2022).[17]

The diffusion of capabilities within the private sector was guided by market mechanisms to build competitiveness (Hong and Goodnight 2019). Rather than the state being in the driver's seat, it worked *with* the private sector to build these capabilities, including through "institutional outsourcing" to private entities (Liu 2021).[18] This is in line with China's overall economic development where, despite its weak institutions, unambiguous goals at the central

[16] The US adopted several policies in response to Japan's rising dominance in the electronics sector in the 1980s. As Japanese firms began to produce semiconductor chips of equivalent quality but cheaper, the US government's efforts to contain its rise, through a floor price to incentivise greater sale of US domestic chips, were somewhat ineffective since it raised prices for the rest of the tech industry even though it favoured the chip industry (Miller 2019). However, the domestic chips industry had a tacit alliance with firms from other countries like South Korea's Samsung to outsource production and bring down costs (Leong 2022).

[17] At the same time, these policies have also led to uneven development in China as the government favoured agglomeration of industrial activities in some provinces to ensure efficacy of its policies (Tommaso et al. in eds. Bianchi et al. 2019).

[18] According to Liu (2021), private entities collaborated with the state to create market institutions, enforce law, conduct policy experiments, facilitate rural development, conduct surveillance and censorship.

level were implemented by a decentralised administrative system where local officials had the autonomy to choose their strategies (Ang 2016).

As many Chinese platforms were encouraged as national champions to counter large foreign (US) giants, they have similarly engaged in data extractivism, which, many argue, has been used to create a 'surveillance state' - extensive use of technology like facial recognition, social credit systems, and widespread internet censorship to monitor and surveil its citizens' activities. Close relations between the state and private firms, who in turn helped build this surveillance state, are not viewed favourably by overseas regulators, with private ownership no longer seen as a credible sign of political independence in China. This has been a key point of contention in the geopolitical rivalry between China and the US as shown by the recent case of Huawei in the 5G rollout (Liu 2021).[19] Nonetheless, the institutional dominance of big tech in China is somewhat similar to the relatively privileged position of private security and defence firms in the US (see above, Huang and Tsai 2022). Rather than Chinese exceptionalism, this points to the crucial role of the state in fostering innovation and growth.

The EU

The **EU** is home to some leading global infrastructure actors, including notably Nokia and Ericsson, as well as mobile operators such as Orange. While the emergence of some of these giants is also linked to a strong role played by the state,[20] the EU has lagged behind in many areas of the digital economy. The emphasis instead on free and fair competition, as mentioned above, is the outcome of several factors such as an open embrace of the neoliberal ideology, as well as its *regional* integration project which has limited space for *national* industrial policies (De Ville 2023). This goes some way in explaining the bloc's regulatory approach.

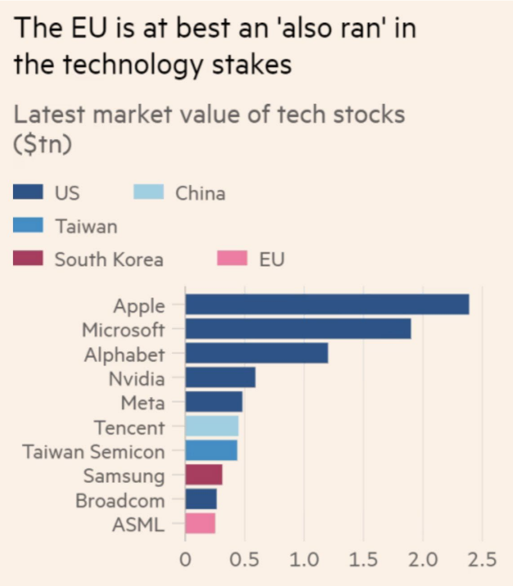
While the EU did institute industrial policies to raise the production of semiconductors in the 1980s, when competition between the US and Japan grew, these policies had limited success. This is mainly because the protection of its technology firms proved insufficient to develop key capabilities, unlike in Taiwan or Japan which had strong private firm conditionalities with strategic decisions taken by public sector agencies (Cobby 2023). The bloc's failure to catch up remains to this day. Nevertheless, the EU does feature in the production of components for semiconductors.

While the EU now seeks to engage in the next phase of development of the data economy, notably the use of industrial data to drive AI, the figures below show that the EU continues to trail competitors in terms of the market value of big tech companies and indeed in AI investment. Some suggest that the gap in the capabilities around artificial intelligence is not as big (for instance, Matthews 2022).

[19] Concerns that the Chinese government could use Huawei technology for malicious purposes including espionage led several countries to ban or restrict the firm in their 5G roll outs.

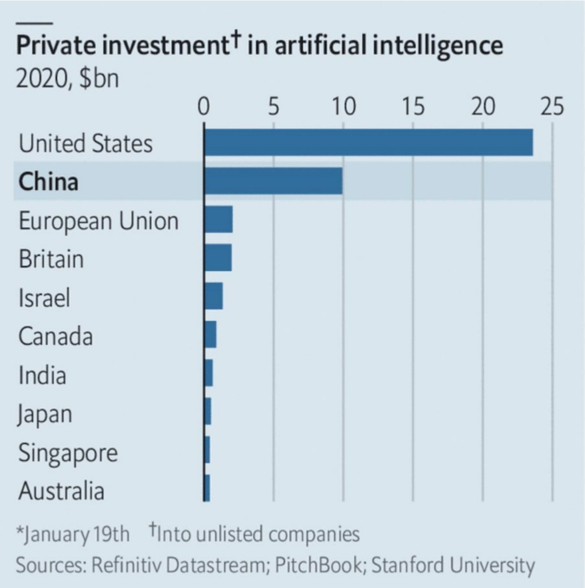
[20] Rather than competition, it was the compulsion of having to pay (in-kind) war reparations to the Soviet Union that explained Finland's phenomenal industrial growth in the post-war period which also led to the rise of Nokia. Its success is partly the result of a merger with other companies where the state-owned enterprise Televa played a leading role in innovating the digital system that formed the basis of the GSM standard, and to some extent by public procurement (Engheim 2021).

Figure 2.1: Leading tech firms are largely non-EU



Source: Wolf 2023

Figure 2.2: The bloc has also fallen behind in investments



Source: The Economist 2022

The EU's current digital industrial policies aim to stimulate the development of European digital champions through more investments, while also focusing on the more traditional functions of industrial policy: to shape the industrial ecosystem and boost firm-level productivity (Timmers 2022). This reflects the bloc's goal of becoming a digital power in its own right, beyond a referee in the global digital ecosystem governance (Hobbes eds. 2020).

Nevertheless, unlike the US where there is bipartisan support for industrial policy, the approach of EU member states to industrial policy differ, with confrontations over the scale and make-up of the EU's upcoming "European Sovereignty Fund".[21] Overall, the EU seeks to catch up with the US and China (Boones et al. 2022), but regulation and policies alone, coupled with existing funds for programmes like Horizon Europe and Digital Europe, may not be enough to spur innovation and get into the ranks of new players like China, in challenging existing US monopolies.[22] Cautionary lessons can be drawn from the experience in the 1980s mentioned above.

2.2. Competition between models

The above section drew on the similarities in digital industrial policy approaches of the established powers even though the motivations behind them are different. But as digital sovereignty becomes a geopolitically charged term, apart from the ambition to develop domestic capabilities, competition over technological innovation is becoming a key aspect of the competition between these established powers, with the difference in approaches to governance becoming another aspect of the rivalry between them. This section will show elements of competition between these models.

[21] The details of the fund remain vague, though the European Commission has hinted that it would like additional resources to finance an EU-wide industrial policy. Internal Market Commissioner, Thierry Breton, has advocated for more common debt and is vocally backed by France, though several Northern member states do not share such enthusiasm.

[22] China invests more in R&D than all of the EU member states put together (Rathenau Instituut 2022). Lower electricity prices ($60-80 MWh compared to $130 in the EU) also help maintain Chinese competitiveness (Yang et al. 2023). Even though wages in China are rising, they are still lower than in the EU. Finally, leading chips and semiconductor manufacturing firms are able to maintain their competitiveness due to their extremely large production capacity and economies of scale.

The US

Geopolitically, the US's economic might, military supremacy and technological popularity have been key to its standing on the global stage. This has been cemented by a strong lobby for industry self-regulation with a push for free digital trade protected by stringent intellectual property protection and a multi-stakeholder approach with US dominance in organisations like ICANN.[23] This approach has bolstered Silicon Valley profits (Mirrlees 2020) with an outsized US influence in this space.

As this hegemony is increasingly challenged by a rising China, there are striking similarities between the current US rhetoric against China and that against Japan in the 1980s (Nymalm 2019). This rivalry is most evidently playing out in the manufacturing capacity of semiconductors. For the US, China's advances in chipmaking threaten its qualitative military advantages that have underscored its power for decades (Kuo 2022).

The semiconductor supply chain is highly specialised with a handful of key players in a few countries engaged in a complex mesh of interconnections (Zhang 2021).[24] Achieving self-sufficiency would be prohibitively expensive even if it were possible, with some experts arguing it is not (for example, eds. Miller 2022). Even so, there is bipartisan support for the $280 billion CHIPS Act in order to boost the US semiconductor industry, with plans to build at least two semiconductor manufacturing clusters in the US by 2030 and reduce its dependence on Taiwan. The IRA provides $370 billion in subsidies for clean energy and has implications for the US semiconductor sector.[25]

While aiming to support domestic industry, these efforts are largely seen as a 'China-proofing' strategy in light of the current geopolitical tensions and tech war.[26] Not only has the US announced several waves of sanctions since 2018 to contain Chinese activities in the area of advanced chip-making, but the CHIPS Act also has extensive conditions on recipients of the funding, such as a 10-year ban on expanding advanced chip capacity in China, among others (Agarwal 2023).

According to Demarais (2022), US sanctions, which aim to clamp down on any exports to China of microchips using US technology closely resemble financial sanctions - they are coercive measures to all firms using US technology, whether they are American or foreign. They essentially force countries and companies to choose sides between the US and China. With virtually every microchip having some link to the US economy, be it because it is designed by US-made software, produced using US-made equipment, or inspected with US-made tools, firms are likely to side with it and stop working with Chinese companies, dealing a heavy blow to China's technological ambitions.[27] At the same time, given the highly intertwined supplier relations, cutting ties with Chinese firms risks severe disruptions in the supply chain and affects other, non-Chinese, suppliers too (Tooze 2023).

China

[23] ICANN creates and distributes top-level domains (.com, .edu, etc.), and used to be closely linked to the US government through oft-renewed contracts with the US Commerce Department since the late 1990s. These domain names have significant political and moral salience and continued US influence in the organisation was deemed a particularly thorny issue, especially in light of the Edward Snowden revelations (Goldsmith 2015).

[24] US controls the higher value-added upstream functions of the supply chain with Taiwan producing the chips, the Netherlands providing lithography machines in the process of chip making, the UK specialising in arm architecture, Japan and South Korea each with their own expertise and it will be difficult for one country to dominate the entire production (Leong 2022).

[25] As the clean energy sector heavily relies on semiconductors, specifically microchips for solar panels, wind turbines and electric vehicles (EVs), the CHIPS Act combined with IRA creates demand for domestic semiconductors.

[26] While the US-China rivalry is also said to be about values, some have argued that such rivalry probably would have been inevitable even if China were a democracy (Luce 2023).

[27] Even firms and countries not falling under the sanctions regime have given in to US pressure as shown in the case of the Dutch private firm ASML (Haeck 2023).

For China, building capabilities in the digital economy is about its economic development, and not just about trade.[28] In order to escape a potential 'middle-income trap', and counter its negative image of engaging in intellectual property theft,[29] China has increasingly focused on building advanced domestic capabilities with support through state intervention - something that developed countries historically practised as well (Werner 2018).[30] The country aims to transform itself from the assembly and manufacture of individual components into a production hub of high-tech products. Policies like "Made in China 2025" have been instituted, influenced by Germany's Industry 4.0 Initiative and US's industrial internet, to foster innovation in ten hi-tech sectors, and complemented by the "Internet Plus" initiative which aims to integrate the internet with traditional industries and manufacturing (Wübbeke et al. 2016). These ambitions are taken further in the 14th five-year plan which emphasises the need to safeguard technological self-sufficiency and strengthen the orientation towards the domestic economy through a strategy of dual circulation.[31]

However, in contrast to the US, China has exercised greater control of online content through an elaborate set of successive measures since the 1990s. This is influenced by its own idea of (digital) sovereignty which rejects Western values (of a "free and open internet") and envisages a greater role for the state (in determining how data is governed within its territory, Creemers 2020). In line with its market-driven but government-led approach, as capabilities in the platform economy grew so did the need for regulation suggesting a shift from market-creating to market-shaping reforms. While the recent spate of regulations[32] wiped out some US$1.5 trillion from Chinese tech platforms (Shen 2021), the trend is not unlike other countries where governments realise the urgency of more stringent regulation on platforms. In many ways, these regulations normalise the digital sector by applying existing rules (e.g. banking or labour laws) to tech platforms (Creemers 2023).

In terms of cyber diplomacy, the DSR is an important tool. It feeds into China's vision of a global infrastructure and trade architecture with a "win-win" narrative - benefitting not only Chinese, including state-owned, firms as they export some of the excess capacity in building infrastructure in China over the decades, along with business opportunities for its digital firms, but also partner countries by building critical infrastructure as they embark on a path to economic development. Apart from that, China has played a key role in shaping global norms and standards by internationalising Chinese national standards while also transposing international ones to the national level (Teleanu 2021). It has also sought to push for reforms in organisations like the ICANN to align more closely with Chinese preferences so as to not be constrained by "rules set by the bully" (i.e. the US, The Economist 2023a).

In general, the Chinese policy stance, reflecting a change from 'hide and bide' under Deng Xiaoping to greater assertiveness (and aggressiveness) under Xi Jinping,[33] is both leading to a more hawkish stance by its counterparts in the US, and to some extent the EU (Gunter and Legarda 2022), and emanating from an increasingly hostile external environment. While the US sanctions have raised the cost and reduced the efficiency of Chinese R&D activity, capital

[28] Its reliance on imports from geopolitical rivals is a matter of strategic vulnerability for its economic development - China spends more than $300 billion on foreign-made semiconductors every year, most of them manufactured with US technologies, making computer chips China's largest import, far above oil (Demarais 2022).

[29] China has been the target of most of the anti-infringement investigations by the US. Research shows that these were more frequent in industries that faced intense import competition (Li and Chen 2020).

[30] Today's advanced countries relied on smuggling and theft when they themselves were developing (Chang 2001). Taking a historical perspective, Werner (2018) points to the problem in the current structure of the global economy by arguing "under the existing form of globalization, the only way to achieve development is to "cheat"—where cheating is defined as significant state intervention in the market economy. The only major countries that have achieved a developmental breakthrough are precisely those that have manipulated the terms on offer by the global economy."

[31] This mainly refers to insulation of the domestic economy from external shocks and bottlenecks, and rebalancing away from (eroding) external demand to domestic demand fulfilled being with domestic production (Herrero 2021).

[32] Since 2020, the Chinese government has introduced several legislations covering fintech and data protection, and online competition (see accompanying note by Musoni 2023).

[33] Domestically too, several analysts have argued that there has been a shift in Chinese state policy from a reformist agenda to a strict loyalty to the head of the party (Rudd 2022).

investments have nonetheless risen in response to US sanctions against Chinese hi-tech sectors, with some experts arguing that in the long term, Chinese companies will overcome the short-term challenges posed by the sanctions (Chen 2023) given the rush to build domestic capabilities in response to the stranglehold of US sanctions.[34] Not only does it view these sanctions as unfair, but it has also been shoring up its military spending perceived by some as threatening the US and leading to a "security dilemma" (The Economist 2023a).

The EU

The overarching European Industrial Strategy, first announced in 2020 and updated during the pandemic, aims to support the EU's twin digital and green transition and "make EU industry more competitive globally, and enhance Europe's open strategic autonomy" (EC n.d.-a).[35] There are specific strategies around data (EC n.d.-b), AI (EC n.d.-c) along with accompanying regulations (for example, the 2022 Data Act, AI Act which is under negotiations) which aim to develop a European data market and to create a thriving AI ecosystem, whilst ensuring high levels of data protection. The Critical Raw Materials Act aims to ensure that the EU has access to the critical raw materials it needs for its twin transition, with a focus on refining, processing and recycling (EC 2023a). The EU Chip Act (in negotiation) is another legislative instrument through which the bloc aims to strengthen its technological leadership (EC 2022)[36] by combining research and innovation with production so that it takes place in Europe (Breton 2022).

In addition, with its regulatory approach, the EU seeks to show a third way to digital sovereignty that contrasts with the US and China by safeguarding personal data. It has put in place digital regulations, and privacy standards, and tried to change the behaviour of big tech firms, including by levying antitrust fines as a third way between the US's surveillance capitalism and China's surveillance state. The Digital Markets Act (DMA), which enters into force in May 2023, seeks to tackle the network effects of large online platforms - so-called gatekeepers - in favour of a fairer business environment for smaller businesses, promote innovation through start-ups, better service to consumers (EC n.d.-d).

This however also calls for a balance between several aspects. In the geopolitical sphere there is also a concern with antagonising the US, which remains a strategic partner but where most of the big tech targeted in the EU legislation are based (Espinoza 2020), or alienating China completely (von der Leyen 2023) which remains an important economic partner, and domestically navigating competing priorities of promoting innovation and at the same time ensuring security and individual privacy (Espinoza 2023). Analysts express concern about the bloc's ability to enable a thriving tech economy given the need to reconcile the facilitation of data flows to boost the tech industry, and stringent privacy restrictions (Burrows and Mueller-Kaler 2021).

The link between the EU's external action and industrial policies is less apparent, though they do exist. For instance, the bloc is increasingly looking at building critical digital infrastructure in partner countries as part of the Global Gateway. This has the potential to strengthen European digital infrastructure actors and to play a role in responding to the infrastructure needs of developing countries. Yet, as we have argued in the past, for Global Gateway to truly respond to the needs of partner countries, it will be essential for the EU to complement these infrastructure investments with support to local research, development and innovation systems that can support the emergence of thriving local digital industries (Teevan and Domingo 2022).

[34] Already China has an edge over the US in 37 out 44 key technologies according to experts (Chen 2023).

[35] There has been some criticism of the term 'twin transition' since the two are not equal twins - digital transition is more a means while the green transition an end (Lema and Rabellotti 2023).

[36] More specifically, it aims to boost research and development capabilities, reinforce capacity to design, manufacture and package advanced chips, build in-depth knowledge of the global semiconductor supply chains, and support the emergence of a skilled workforce (EC n.d.-e).

The US's IRA has further propelled a subsidy race that was already heating up, leading the EU to announce a Green Deal Industrial Plan (GDIP) (EC 2023b) to boost its own green and digital industry, and fortify the EU's strategic autonomy. In seeking to respond to what is essentially a US response to China's ascension, the EU is joining the club of big nations that have recently announced similar industrial policies (Detsch 2023). Even though the target of the IRA is specifically green industries, as mentioned above there is a link to the digital sector, and therefore implications for the EU's twin transition. Yet, the new GDIP does not have many fresh resources and rather refashions existing resources (Stolton and Haeck 2023), including the not yet exhausted Next Generation EU COVID-19 recovery package. Moreover, given the inherent challenges of managing a confederation of states and the EU's lack of considerable own resources, recent policy interventions have focused on a relaxation in the otherwise tight state aid rules at the national level rather than awarding subsidies at the European level (Wolf 2023). As these policies tend to be more national than European, they risk greater inequalities as countries with greater fiscal space will be better placed to undertake such endeavours (Ibid).

2.3. Implications for developing countries

Section 2.1. highlights the key role for (digital) industrial policies with a prominent, though varying, role played by the state. This is in contrast to developing countries where for many years governments have largely been instructed that people are best served through market forces (Said 2021). By advocating a very limited role for the state, given the bad track record of governments to 'pick winners', industrial policies have remained largely absent in many developing countries since the structural adjustment programmes of the 1980s. Consequently, not only are low and middle-income countries using industrial policies to a lesser extent - despite the fact these will be indispensable for their development - compared to high-income countries, but these states also lack the fiscal and administrative capacity to deploy them (Juhász et al. 2023).

Most developing countries lack the capabilities to build their own digital hardware and software. Instead, the greatest advantage of the digital economy lies in the ability to absorb available technologies to increase output and productivity in agriculture and manufacturing value chains.[37] However, this too requires dedicated digital industrial policies that foster local innovation and/or create demand in the domestic private sector given the challenges of absorptive capacity. This in turn requires coordination across firms and sectors to promote backward and forward linkages. As we will explore in later sections, in India in particular, and in Africa to some extent, there is a renewed interest in industrial policy.

Many developing countries also face the risk of digital colonialism where digital technologies are used for "political, economic and social domination of another nation or territory" (Solon 2017; Kwet 2021).[38] With countries relying on foreign technologies to build critical infrastructure as well as raise productivity, there are questions around what digital sovereignty means in such a context. Given limited alternatives, countries aim to spur local innovation by expanding internet access through, ironically, partnerships with precisely the giants that engage in data extractivism, as they increasingly integrate vertically and reduce the cost of their service provision (Mims 2022) and despite security concerns (Ehl 2022). At the same time, unless firms are able to absorb these technologies to raise their productivity, the gap between firms in the Global North and Global South is only likely to widen (Lema and Rabellotti 2023).

[37] While many developing countries seek structural transformation through industrialisation and integration into global value chains, they can no longer rely on low wages alone. In fact, lead firms often search for suppliers who are ready to adopt frontier technologies in order to maintain their competitiveness and market share (Lema and Rabellotti 2023).

[38] For instance, applications like Facebook have most of their users (over 90%), from whom they extract data, in countries outside the US. Similar concerns are also raised about Chinese applications like TikTok. While data extraction can be used for machine learning and improvements in user experience, among other things, it can also have undesirable effects including the replication of exploitative colonial relations through a new form of resource appropriation (namely of data, instead of land and labour during colonial times).

The competition among established powers as highlighted in section 2.2. also presents challenges to developing countries. While the US push to move supply chains away from China may create opportunities for some countries, notably India, it may also have negative repercussions for others whose relations straddle multiple blocs - especially in Africa - and who are reluctant to pick sides (Munga and Denwood 2022). In many countries, China plays an important role in building digital infrastructure (5G, cloud computing among others) with its investments in Africa surpassing that of all multilateral agencies and other bilateral donors combined (Arcesati 2020). With geopolitical rivalries playing out in Africa, it would be important to avoid a situation of distinct tech spheres that are decoupled due to security concerns emanating from US-China tensions, especially in light of African own (continental) priorities of a single digital market (Nyabiage 2022). This reflects limited policy space given that market access to partner countries such as the US or the EU may be dependent on certain decisions and policy choices.

Furthermore, the emerging subsidy race can be especially detrimental if it takes away those investments which could potentially have been developed in these countries - such as refining of mineral inputs for semiconductors and microchips. Constrained by rising costs of borrowing, and saddled with a high debt burden, these countries have limited fiscal space to compete with giants such as the US, the EU or China. More poignantly, "...if the United States and Europe agree to discriminatory manufacturing subsidies, and only China can afford to compete, it tells the rest of the world that their aspirations for development do not matter" (Posen 2023). Indeed developing countries, especially in Africa, risk facing green/digital "apartheid" where opportunities and access are segregated by race and geography while reinforcing colonial structures of raw material exports (Moss 2023). Thus in trying to penalise their supposed adversaries, subsidies of established digital powers may hurt developing countries with a risk of growing resentment (Harris 2023).

3. Rising powers

As competition among these established digital powers unfolds, there are rising powers which are charting their own course of digital development. Typically they do not have a broad foundation of sufficient infrastructure, strong regulatory capacity, or well-developed eco-systems on which to base their digital strides (eds. Pannier 2023). Internet usage is mainly through mobile use, and in many cases, digital policies are centred around increasing access and leveraging it for economic growth and development (Domingo and Tadesse Shiferaw 2022b). Indeed with vast informal sectors and low levels of mechanisation, to a large extent firms in developing countries are yet to achieve the stage of Industry 2.0 which involves electrification and mass production through assembly lines or Industry 3.0 which involves partial automation of the production process with the use of computers before they embrace Industry 4.0, where ICT is applied to production for smart manufacturing (Lema and Rabellotti 2023).

The above digital powers - the US, China and the EU - influence the way the digital industrial policies in these countries have evolved. In the larger geopolitical race between the US and China, these countries increasingly find themselves in a difficult position where they either choose Chinese firms and risk ties with the United States or ban Chinese firms and invite repercussions from China (Pant and Tirkey 2021). In an effort to navigate these stark choices, they adopt a path of pragmatism with fuzzy blocs in order to retain market access as well as benefit from partnerships with the different geopolitical powers (Higgott and Reich 2022). We look specifically at India and Africa as a whole.

India's digital public infrastructure

India's approach to digital sovereignty seeks to balance the digital 'trilemma' of generating economic growth which hinges on data access, protecting individual privacy and safeguarding national security (Saran 2016). Security threats from China, combined with equally complicated, if less fraught, relations with the US have created an urgency to forge its own path and, more importantly, avoid becoming collateral damage in the rising US-China tensions. Increasingly positioning itself favourably to take advantage of the opportunities provided by the global shift towards a "China plus one" strategy, India is among the few countries outside the established powers with readiness to adopt digital technologies (UNCTAD 2020). In navigating these realities, India aims to become a bridge between the Global North and the Global South. Indeed its approach, neither excessive state intervention nor exclusively laissez-faire, has encouraged innovation.

A key feature of India's technological advances is its digital public infrastructure, embodied in the 'Digital India' initiatives which aim to provide digital government services. This includes India Stack which is a comprehensive digital identity, payment, and data-management system.[39] Feeding into this digital infrastructure are innovations using free and open-source software (FOSS) where the country has created a certain niche and which has allowed for building local capabilities. Not only is there a dedicated policy on the adoption of FOSS since 2015, but the government has also played a key role in spurring this activity through large-scale projects like the universal ID (Aadhaar) system that forms a building block of India Stack. The Unified Payments Interface (UPI), which allows for an ecosystem of multiple payments systems to interoperate, is also a second building block of India Stack and is under the oversight of an umbrella institution to operate retail payments and settlements, backed by the central bank of the country - Reserve Bank of India (Kearns and Mathew 2022).

Allowing aggregated, non-personalised, data in the public domain under the third layer of India Stack, though aggregators that intermediate data flow between firms and individuals, has allowed for innovations in tech applications in other sectors like health, education, rural livelihoods, pharmaceuticals, among others, thereby spreading the benefits of digital technologies more widely into the economy and society (UNCTAD 2020). Data sharing is also being leveraged to design efficient transport and logistics systems to boost economic growth (The Economist 2023b). Apart from these government-led initiatives, several multinational companies, including tech giants like Alphabet Amazon and Microsoft and manufacturers deploying digital technologies e.g. Boeing, Walmart, and Rolls-Royce, among others have, or plan to, set up R&D centres to tap into the pool of educated workforce combined with lower wages (The Economist 2023c). The country also boasts the highest number of unicorn start-ups[40] (115) behind the US (661) and China (312) (Mitter 2023).

Yet, India has seen limited success overall in scaling up private sector investments to build domestic capabilities in digital hardware and software. It has seen greater advances in specific aspects, such as the 5G rollout, where Indian telecom operators also participated. While the Indian government sought to address security concerns over its reliance on Chinese equipment providers by working with other foreign firms,[41] it also came at a greater cost - the highest among emerging nations according to a recent study (Economic Times 2022), with these other providers, unlike their Chinese counterparts, not providing end-to-end services. Nevertheless, the government has introduced initiatives to promote manufacturing capabilities in the country.[42]

[39] India stack has multiple layers namely digital identification which includes i) a two-step verification process of the ID and biometrics, ii) interoperable payments system, verification of digital documents to enhance efficiency and integrity, and iii) intermediation of the flow of data between individuals and firms (Carrière-Swallow et al. 2021).

[40] Unicorns are private start-ups that are valued at over US$1 billion.

[41] In order to reduce its reliance on Chinese providers for its critical infrastructure and ensure cybersecurity, India announced 5G roll out trials with Ericson, Nokia, Samsung and C-Dot equipment in an effort towards vendor diversification, but without explicitly banning Huawei and other Chinese equipment providers (Pant and Tirkey 2021).

[42] Government initiatives to promote electronics manufacturing include Modified Electronics Clusters (EMC 2.0), Scheme for Promotion of Manufacturing of Electronic Components and Semiconductors (SPECS), Program for Development of Semiconductors and Display Manufacturing Ecosystem, Production-Linked Incentives (PLIs), among others (Ray in eds. Pannier 2023; Cyrill 2023). In addition, the Make in India initiative aims to attract manufacturing investments into the country, including, but not limited to, electronics (Chaudhuri 2021).

Despite these measures and its large internal market, the Indian market is also constrained by the lack of a steady supply of *skilled* labour coupled with onerous labour regulations, infrastructural bottlenecks notwithstanding recent improvements as well as delays due to bureaucratic red tape (EIU 2023). Moreover, it faces stiff competition from other emerging markets in Southeast Asia.[43]

Nevertheless, its digital performance compared to its income level (UNCTAD 2020) provides an attraction of the 'Indian model' to its peers in Africa. Its strides in technological uptake place India in a unique position to also access overseas markets (EIU 2023). For instance, India has, or plans, cooperation agreements with Sri Lanka (Hersey 2022; Fernando 2023), Philippines (Macdonald 2022), Singapore (MAS 2023), and several African countries including Morocco, Tanzania (Phartiyal 2023) to export its technology for biometric identification and digital payments. The country also exercises digital diplomacy by advocating for multilateralism, encouraging its experimental approach and open-source innovations, and increasingly working towards building the capacity of the state and netizens to counter misinformation through cyber hygiene (MeitY 2018).

African countries' effort to seize digital opportunities in global value chains

Given their socioeconomic needs and institutional capacity, economic independence and development for African countries in the digital economy looks very different to the above cases. The vast digital divide, like in India, means that the focus of most governments is on expanding access to the internet for its population, which is limited to 28% compared to 82% in the EU and the US (Orufa 2023) and with significant differences between urban and rural areas. However, this is also a diverse continent with different starting points in terms of digital capacities across countries.

Consumption of digital technologies by consumers, which is how Africa's digital revolution is often framed, is different to the production of value by African businesses by harnessing technologies (Mann 2016). Only a few African alternatives exist to improve connectivity across the continent (Orufa 2023), though there have been innovations in the financial sector (for example, M-Pesa) and others like transport, health, digital lending and agriculture (Mutung'u in eds. Pannier 2023). In many ways, though, the propagation of these technologies is seen as part of a social rather than an industrial policy.[44]

The nature of globalisation has shifted in that trade is less about goods and services and more about data which has also become a strategic asset for firms that is accumulated, exchanged and analysed (eds. Bianchi et al. 2019). This in turn means higher barriers to entry for African firms, as they lack infrastructure and connectivity, as well as skilled human resources and know-how (Banga 2022).

In order to take advantage of the opportunities provided in the digital tech space, Swaniker (2023) makes a useful distinction between tech products and tech services. While innovation in the tech product space could result in some African champions (rivals to Netflix, Meta, Google, Microsoft, Amazon, Apple, Spotify, TikTok, etc.), these firms normally employ few, but highly-talented, people and operate under pressure to turn profits backed by short-term venture capitalist funding, with a high rate of failure. Firms in the tech services space, on the other hand, employ 100-300 times more workers, mostly at the entry level, to train them, therefore, bringing greater benefits in terms of employment and entails lower risks. This calls for different strategies, with the longer-term public investments in research and innovation, as well as education to build the right skills in the workforce.

Digital development is also about harnessing available digital technologies to collect data along the entire value chains to raise productivity (Andreoni and Avenyo 2021). Currently, however, such technology adoption remains

[43] Malaysia has a strong electronics cluster, and Thailand has a competitive automotive manufacturing sector, while Vietnam has already successfully attracted value-added manufacturing that left China. Moreover, the efficiency of the supply chains that still remain in China is also attractive to investors (EIU 2023). A good example of this is Apple (McGee 2023).

[44] For instance, digital government payments for financial inclusion (Desai et al. 2022).

extremely limited - Nigeria, Kenya, South Africa and Egypt alone account for 92% of total investments in the digital technology sector in Africa (Okunoye in eds. Pannier 2023). Despite relatively high technology adoption in these countries, it does not include advanced technologies, much less 4IR or smart manufacturing applications.[45,46] Firms that do adopt these modern digital technologies are unable to establish backward and forward linkages within the domestic economy (UNIDO 2019; Lema and Rabellotti 2023). North African countries aim to overcome this challenge by taking advantage of their proximity to, and relatively advanced integration with, the EU Single Market through European value chains (El Aynaoui et al. 2022). Digital technologies can also be applied to less complex manufacturing to improve efficiency and reduce unit costs. On the other hand, countries such as Kenya have tapped into global value chains with some opportunities in data processing services, though these are mainly low-end activities.[47] Nevertheless, Africa's share in the global digital economy (proxied by the sale of robots) is 15 times lower than its overall GDP share (Banga 2018).

There are many challenges to adopting digital technologies - lack of infrastructure including energy, skills, and financing but importantly a productive base in which to adopt these technologies. Thus, digital industrial policies in Africa should prioritise an expansion in the productive base for greater value capture as well as the adoption of digital technologies in manufacturing (Ibid.). This requires a balance to ensure that dependence on foreign technology does not translate to anti-competitive behaviour or have negative labour implications as observed with the platform economy (Kleibert and Mann 2020).

Despite these more developmental concerns, digital connectivity and governance remain a geopolitical issue. The rush to connectivity has been led on the one hand by the big tech (for example, erstwhile Facebook’s Free Basics) and China’s Digital Silk Road on the other. Concerns of intellectual monopoly and digital colonialism have led to several countries adopting data localisation rules (see Musoni 2023 in this report).

As many African countries view regulation of cross-border data flows as a way to build domestic capabilities in digitally-intensive sectors (Atabey in eds. Sampath and Tregenna 2022), these policies should be used to discipline domestic firms and encourage innovation. In this regard, too many restrictions on flows can also impinge on data access for innovation and productivity gains. Thus there is a need to balance security concerns with the objective of using data to spur economic growth as shown by existing case studies (Adeleke 2021).

Even though there is currently no common framework to govern data flows, the new AU Data Policy Framework (AU 2022) and the Africa Continental Free Trade Area (AfCFTA) could be vehicles through which countries seek harmonisation in policies to promote greater digital trade (Chivunga and Tempest 2022; Beyleveld and Sucker 2022). Countries are championing continent-wide programs like Smart Africa Alliance and Africa Digital Content and Innovation Program. For instance, under this initiative, the Government of Kenya is playing a leading role in designing a national digital economy strategy which can be a guide for others. Already the continent is moving towards an interoperable cross-border digital payments infrastructure through the Pan-African Payments and Settlement System (PAPSS) (Teevan 2023) which is an integral part of the AfCFTA. The ambitions for developing manufacturing

[45] In Kenya, 44% self-employed business owners use digital services but only 15-18% use advanced digital services (Domingo 2023) such as keeping business records and track stock, buying/selling supplies/products through e-commerce platforms, using digital governance services to register businesses and pay taxes and levies (Koyama et al. 2021).

[46] A recent survey of 500 companies in Ghana showed that over 90% of the firms had analog or rigid production systems with adoption of specific digital technologies such as robots, cobots, 3D printing, big data, and augmented/virtual reality being very low at 3.6%, 5.2%, 5.6%, 9.6% and 4.6% respectively (Lema and Rabellotti 2023). Figures in the EU stand at around 45%, 25%, 15% and 30% respectively (EIB 2019).

[47] Lead firms dominate high end value adding activities and enjoy concentrated market power in the provision and production of intangible assets, also called “intellectual monopoly”, with negative socioeconomic implications for the development prospects of developing countries who only perform low value-added activities as depicted by the smile curve (Durand and Winkler 2018). In addition, labour relations have been a concern as seen in the case of ChatGPT moderators, with a recent lawsuit against Meta in Kenya (Komminoth 2023; Ogunjuyigbe 2023).

in the continent are also reflected in the recently concluded Transform Africa Summit, where Heads of State emphasised the need for African solutions.

4. Conclusion/policy recommendations

This chapter has discussed the way the digital economy has been shaped by industrial policies among the established and rising powers. While for different motivations, there has been borrowing and learning from the ‘other’, for instance, China’s learning from the US experience, even if this has led to retaliation, for instance US subsidies to contain China, and EU subsidies to match up to the US. The current global landscape of digital strategies and policies is characterised by the coexistence of multiple models with related industrial policies adapted to respond to these needs.

Even so, the way industrial policies have been used is not very different in the cases discussed. For instance, in all countries, the role of the state has been crucial in giving direction for innovation and shaping markets, though admittedly this is done for different purposes. For instance, in the US this was/is for security and defence purposes, while in China it was to create national champions and spur economic growth to become a high-income country. The EU on the other hand, seeks to chart a way for the ethical use of digital technologies, while India’s industrial policies reflect the creation and exploitation of the niche for domestic innovation to provide an alternative that is more applicable to the development context in most of the Global South.

As these powers increasingly project their soft power externally, they can also be seen as an extension of domestic industrial policies. While they are meant to give other developing countries a pallet of options to choose from when looking at their specific local circumstances, increasingly, the space for countries to make such independent choices, without it being interpreted as a sign of political or security loyalties, is reducing. Moreover, as the current subsidy race unfolds among established powers to maintain or create global hegemony over digital technologies, it risks creating an even greater rift between the rich world and the rest who do not have the fiscal space and financial might to support the development of their own industries.

The implications of digital industrial policies among established powers on developing countries is far reaching. Though the innovation as well as adoption of modern digital technologies is concentrated among few advanced countries and China, developing countries must harness digital technologies to improve their production systems if they want to remain integrated in the global economy. This calls for a dedicated digital industrial policy to facilitate and coordinate the absorption of these digital technologies. At the same time, stronger regulations are needed in order to mitigate some of the negative impacts of the big tech firms and the platform economy, while balancing these with the development needs. Lessons can be drawn from the established as well as rising powers in this regard, in order to sequence reforms in a way that first create and shape domestic markets before fixing them.

Chapter 3 – Integrating digital sovereignty in EU external action by Chloe Teevan and Ennatu Domingo

1. Introduction

The EU increasingly refers to digital sovereignty both domestically and internationally, and yet there is still quite a lot of ambiguity about precisely what this term means to European stakeholders, and indeed whether they share the same vision. The European approach is multifaceted and encompasses a wide range of regulatory measures, coupled with a growing focus on industrial policy. There is a strong focus on individual rights, while at the same time, there is a growing focus on supporting European businesses. The concept is also increasingly evoked in EU foreign and security policy, as well as in the EU's wider international partnerships, but it is not entirely clear how this approach carries over to EU external action. The EU remains somewhat vague about defining this term when using it at multilateral fora or in its relations with other countries.

This chapter looks at how the EU might develop a new approach to digital sovereignty at the international level, working more closely with others in a collaborative and open-minded way. The EU would need to better demonstrate how its policies back up its promise of supporting digital sovereignty in partner countries, and ensure that its domestic policies are consistent with its international rhetoric around developing more respectful and mutually beneficial international partnerships. At present, there is a great deal of geopolitical competition around investments and international partnerships with developing countries in the Global South. If the EU is seen to be preaching and trying to externalise its vision and regulations, this may ultimately be counterproductive and may give rise to accusations of neocolonial practices. This means that the EU should work with others to come up with a shared basic understanding of this term. This chapter aims to lay out some of the ways that the EU might approach this exercise.

This chapter draws on interviews and ongoing conversations with policymakers, academics and analysts, mainly in Europe, Africa and India. It also draws on a range of EU and partner country policy documents, academic literature and the work of other policy researchers. In the first section, it looks at different approaches to defining digital sovereignty within the EU. It then moves on to look at how the EU might better integrate the concept of digital sovereignty into its external actions, identifying some key dimensions of a new approach. In the third section, it looks at how the EU can work more closely with partner countries, particularly in the Global South to come up with common approaches to digital sovereignty, and in the final section, it summarises some of the arguments contained in the paper and some of the recommendations that these arguments lead to.

2. Defining Digital Sovereignty

As previously mentioned, although the term is widely used, the term digital sovereignty is rarely defined in most EU policy documents. However, in the European Council Conclusions of October 2020, the following quite broad goals were laid out to make the EU digitally sovereign: "To be digitally sovereign, the EU must build a truly digital single market, reinforce its ability to define its own rules, to make autonomous technological choices, and to develop and deploy strategic digital capacities and infrastructure." This development should follow a human-centric approach that would "safeguard our values, fundamental rights and security, and be socially balanced" (EUCO 2020). To pave the way for its digital sovereignty, the EU outlined its strategy in the Digital Compass, a ten-year roadmap for Europe's digital transformation. It aims to both build on Europe's strengths, including its single market, its values and its educated workforce, while also addressing "any strategic weaknesses, vulnerabilities and high-risk dependencies." (EC 2021a).

Yet as a number of analysts have previously pointed out, there appear to be a number of divisions between EU policymakers with regard to the essential element of digital sovereignty, and there are a number of tensions in the ways that different policymakers define the term. Pons points to a tension between the French and German approaches: 'France defines digital sovereignty in terms of infrastructure, while the Germans prefer to talk about data sovereignty (Datenhoheit). For Germany, sovereignty is a barrier to the export of its goods, whereas France thinks it is a protective barrier for its values.' (Pons 2023) Others have also pointed to the tension between a definition that focuses on individual sovereignty versus collective sovereignty in the EU approach (Bauer 2020). Indeed, for certain theorists, the EU should not attempt to construct European giants through a reinforced state role, but should rather invest in creating a democratic policy on digital sovereignty by ending the monopoly power of big tech through reinforcement of competition policy (Rimbaud 2021).

Yet, as discussed elsewhere in this report, the EU is taking a two-prong approach to digital sovereignty, which has accelerated since the beginning of the von der Leyen Commission in 2019. On the one hand, it is looking to increase the robustness of its regulatory toolkit through the adoption of a host of new policies and laws with the aim of creating a more democratic and competitive digital environment. On the other hand, it has begun to gradually embrace an active digital industrial policy, hoping to stimulate the development of European digital champions through more investments in the digital sector (See chapters by Musoni and Karkare in this report). At the heart of the EU's regulatory approach is what it refers to as its human-centric vision of digital governance. Commission Executive Vice President Vestager, when launching the European Declaration on Digital Rights and Principles for the Digital Decade, highlighted that the Declaration would be the cornerstone of the EU's human-centred digital policy: 'We believe in a human-centred digital transformation. A transformation where no one is left behind. We want safe technologies that work for people, and of course that our rights and values are as well respected online as they are offline. And we want everyone to be empowered that we as citizens feel that it is our society, that we feel empowered to actively to take part.' (Vestager 2022).

3. Key dimensions of a new approach

The EU Commission started using the term 'digital sovereignty' in its external action as early as 2016, in the EU's 'Global Strategy for Foreign and Security Policy,' linking it to its concept of 'strategic autonomy.' (EEAS 2016). The July 2022 Council Conclusions on Digital Diplomacy highlight the importance of a more robust digital diplomacy to support the EU's "ambitious quest to strengthen its technological and digital sovereignty." (CoEU 2022) These efforts have been most apparent in the EU's recent efforts to proactively influence global standards through stepped up diplomacy at multilateral fora, and by leveraging its position as one of the world's largest markets with the 'Brussels Effect' - its capacity to shape or align regulatory environments outside of the EU to its domestic policies and regulations, initially via market mechanisms (see Musoni in this report). Meanwhile, the Global Gateway Strategy, with its focus on sustainable and trusted connections with the rest of the world, does not explicitly mention digital sovereignty, but makes clear that it hopes to provide partner countries with "secure and trustworthy digital infrastructures and technologies underpinned by proper regulation," thereby echoing some of the elements at the heart of the European approach to digital sovereignty (EC 2021b).

Yet beyond these specific external-facing measures, the EU also needs to begin to demonstrate that there is consistency between the concept of digital sovereignty in its internal and external policies in line with the aims of the so-called "Geopolitical Commission" (Teevan and Sheriff 2019, Teevan 2019). It will also need to show an openness to compromising with partners across the world, working with them to come up with common approaches to key concepts that are central to the European approach, including developing an inclusive approach to "human-centric" digital transformation. Further, the EU will need to demonstrate how its approach to data governance and to digital governance more broadly can be meaningful to others, and again show an openness to new approaches and to compromise.

3.1. Consistency between internal and external policies

An essential element will involve developing greater consistency between internal and external policies. Thus, the approach to digital sovereignty in external action would need to both; 1) integrate an understanding of the external dimension into laws and regulations that aim to strengthen Europe's domestic digital sovereignty; and 2) take into account the indirect impacts or implications of EU domestic policies for partner countries. The external dimension should be considered in all new domestic digital and industrial policies, including both how to mitigate harms and to extend benefits (for example, Digital Services Act, Digital Markets Act, AI Act, Cybersecurity Act, EU Chip Act, etc.).

In external action, the EU is currently strongly focused on creating digital norms and standards as one of the key elements of its digital sovereignty model (Burwell and Propp 2022), and yet the external dimension of new policies is not always sufficiently considered in the texts of new policies and laws. The EU is keen to promote the so-called "Brussels effect" through its digital diplomacy and international cooperation. For example, the EU hopes that the recently adopted Digital Markets Act (DMA) and the Digital Services Act (DSA) will increase the influence of the internal market and its regulatory power internationally (Broeders et al. 2023). Yet, the positive external impact of these new laws is assumed rather than studied in-depth. For example, in the impact assessment for the Digital Services Act, a short section on "Trade, third countries and international relations" briefly discusses the obligations that the Act would place on third country service providers, whether the proposals are in line with international obligations and includes one paragraph on the potential impact on relations with third countries. However, while it hints at the potential for this Act to put the EU in a leadership role, it does not really consider how this might be achieved and the wider potential impact for third countries, including notably in the Global South (EC 2020a).

There is a need to integrate the external dimension into all domestic strategies and to carry out real impact assessments with regard to the impact of domestic regulations externally. While it is understandable that the EU is eager to move quickly with new regulations designed to protect its citizens and to improve the competitiveness of its single market, a greater consideration of the external impact of new regulations would demonstrate a less unilateral approach. Taking into consideration potential impacts on partner countries amongst the least developed and lower-middle income countries would be particularly important in order to ensure coherence with EU development policy goals.

At the same time, the EU should pay attention to the indirect impacts of domestic policies, notably around industrial policy, and not ignore the potentially negative impacts. The EU's rhetoric vis-a-vis partners in the global south largely ignores the ongoing technology race - and consequent subsidy race - taking place between established powers that may leave the global south even further behind (See Karkare 2023 in this report).

The EU should thus clearly lay out ideas about how its growing focus on domestic industrial policy can also integrate partner countries' interests and ambitions. The EU should try to integrate partner countries into new initiatives in a positive way in line with their national development ambitions, including potentially integrating them into European value chains, thereby showing the real benefit of partnering with the EU. There are hints of this in certain policies, such as the recently published Critical Raw Materials Act (EC 2023a) that aims to support partners "to promote their own economic development in a sustainable manner through value chain creation in their own countries" alongside the aim of creating diversified value chains for the EU. Another interesting example is EU support to the AU's Data Policy Framework, with its aim of creating an African data market. Yet, there is room to be more deliberate about this.

In order to ensure follow-up on these policies, the Global Gateway should gradually develop a stronger focus on industrialisation, supporting local technology hubs and funding research and innovation partnerships (the vaccine manufacturing hubs are a good example in another sector). New EU policies should be supported by realistic projects under the Global Gateway, such as the aforementioned investments in critical raw materials processing hubs under the EU's Critical Raw Materials Act. It will also be important that the Global Gateway is not limited to supporting the externalisation of EU industries, but that it plays a role in supporting the development of local industries through research and innovation partnerships, integrating local players into value chains, and allowing for a certain amount of technology transfer. This might include further efforts to support joint research and to stimulate innovation partnerships between businesses in Europe and the Global South. This might include reinforcing Horizon Europe's external dimension and extending the Digital Europe programme beyond Europe's borders, and potentially integrating a wider number of countries into some of its initiatives.

3.2. A common understanding of 'human-centric' digital transformation

As mentioned above, the EU aims to promote its vision of digital sovereignty based on what it calls 'human-centric' digital governance, and it has increasingly been referring to this in various policies on digital for development and at multilateral fora. Although this term is widely used by a number of different international actors, it remains very unclear as different actors understand and see that they can promote it in different ways such as through digital governance and data protection or through increasing investment in digital infrastructure. The EU has started to increase its engagement on the human-centric approach to digital governance, including via the appointment of a Digital Affairs Officer at the EU Delegation to the UN in Geneva, by bringing up the concept at multilateral fora such as the ITU and by calling for stronger partnerships for more inclusive, secure and sustainable digital transformation and opening a new EU office in San Francisco to strengthen digital cooperation with the US (Teevan and Domingo 2022: EEAS 2022).

The EU can lead discussions to develop a common understanding of the concept rather than imposing its own term after it has found a common and clear European view and clarified how it will operationalise the concept (CONCORD 2023). There are already good examples of how the EU is building digital partnerships based on similarities around this concept, as it seeks partners to create and shape global standards on internet governance. For example, in 2020, during the EU-India Summit, which gave the EU-India partnership a more strategic dimension, the EU and India agreed to 'harness human-centric digitalisation to develop inclusive economies and societies', marking the first time that the terms were used to refer to their ambition to enhance convergence between their respective regulatory frameworks to ensure the protection of personal data and privacy (EC 2020b).

Given that there are multiple digital governance models, the EU's concept of 'human-centric' digital transformation is a distinctive mark that is used to help the bloc to differentiate itself from alternative offers. However, the EU should embed its human-centric approach to technology in its partnerships as well as multilateral organisations with concrete definitions. Civil society organisations have even suggested to exchange the term 'human-centric' to 'people-centred' as an attempt to help narrow the scope of the concept to make it more implementable and measurable (ETGovernment 2023). A study conducted by CONCORD states that it is better to refer to "people-centred approach" rather than to a 'human-centric approach' because it is a term that best reflects the value of each individual person. They claim that the concept 'Human' is neutral and disconnected from individuals. Although Amnesty International has raised concerns that 'people' as a category defined by states (for example, China) can result in the prioritisation of economic groups' interests over individual's rights and exclude them from necessary consultation processes (Amnesty International 2023), the term "people centred" can be found in AU policy documents (alternated with ‘human-centred’ or ‘user-centred’ digital technology) and in UN initiatives, and thus may also provide an interesting basis for negotiation with third countries. A letter following the 2021 High-Level Digital Debate of the General Assembly on Connectivity and Digital Cooperation, signed by a mix of actors from the private sector, international organisation and civil society in Europe, the US and the Global South called for: “the international community to put people at the centre of our approach to ensure no one is left behind without affordable access, skilling, and basic public services.” (UN 2021).

The AU Digital Transformation Strategy, focused on deepening digitalisation for development, uses the term ‘people - centred digital transformation’, which is a starting point for a common view on the concept. Nevertheless, while at the regional level, the strategy stresses that ‘any capacity development effort to digitise the African society must be people-centred….’, at the country level, economic needs might be prioritised over the need to protect citizens and their data. Understanding the bargaining process between economic needs and human rights will be essential as the EU promotes a ‘human-centric’ digital governance model including the benefits of strong data protection.

To promote its vision of human-centric digital transformation, the July 2022 Council Conclusions on strengthening the EU’s Digital Diplomacy set commitments for the EU to expand its network of diplomats on digitalisation and to improve coordination with its member states. The EU has made significant progress in its bilateral relations with the US and at multilateral fora. **Yet, it needs to accelerate its digital diplomacy vis-a-vis developing countries to build more significant digital partnerships across the world.** In Africa, as part of the programming of the Neighbourhood, Development and International Cooperation Instrument - Global Europe (NDICI - Global Europe), most EU delegations improved their capacity by appointing focal points to act as their experts on digital policy. These could be coordinated under a regional framework for a more coordinated engagement with African digital partners on digital questions.

3.3. Data sovereignty as data for public good

The EU’s data governance model emphasises citizens’ and businesses’ control over the data they contribute to generate, based on fundamental values and fundamental rights in all data-sharing. As Musoni discusses in her chapter, the EU’s GDPR sets high data adequacy standards for businesses targeting EU consumers, which prevents countries that do not match the GDPR’s requirements from entering the EU market. But many countries do not ensure the same level of protection for European businesses and citizens as the GDPR requires. For many developing countries, it may be difficult to achieve these levels of data protection, while for others competing interests mean that they may prefer to only partially replicate the EU’s model. This has led to countries questioning the EU’s approach, thereby looking to alternative options that are more flexible and context-based. This means that in order to continue to have the widest possible influence in the area of data protection - and in other areas of regulation moving forward - the EU should adopt a more flexible approach that embraces multiple strategies.

To promote its vision of data sovereignty, the EU should understand that a very strict approach to the adoption of its regulatory framework might go against its geopolitical ambitions given its partner’s diverse social values and economic realities. In India for instance, there is a clear interest to collaborate with the EU to set global standards on digital governance and to ensure an open, free, stable and secure digital space, even if there are differences in their data protection policies, especially on the issue of ownership of data. Since the launch of the EU’s GDPR in 2016, there has been strong criticism about the EU imposing its view of data protection on third countries. This resonated in Africa, where governments have been developing national data protection laws but that are far from being ready to fully comply with the GDPR data obligations (Mannion 2021). Some African governments simply don’t have the infrastructure nor the expertise to do so. Even if many African governments agree on the principles under the GDPR, poor implementation of data privacy laws has weakened the protection provided and limited innovation needed to support economic growth and development.

Together with continuing to play a role in shaping data protection and privacy norms by expanding its partnerships, the EU should support its partners in developing their own approach to regulating the use of data in a way that also carefully accounts for local priorities, needs and capacities (Pisa and Nwankwo 2021). An increasing number of African governments are developing data protection policies to respond to local needs (for example, attract investment, as well as address the abuse of data of vulnerable communities which is becoming a domestic issue) as a result the discourse around data privacy has increasingly been focusing on the idea of basic rights. Yet, discussions on the externalisation of the GDPR have revolved around difficulties in implementing the EU's regulatory framework, challenges for data protection authorities to comply with its principles, and the responsiveness of the regulation to partners' social and economic values. This means that the EU's success in promoting its data sovereignty lies in focusing on how it can support the development of data protection policies that promote the growth of local economies and that can ensure a win-win solution. This is especially important for partners that are looking at the EU model but operate in resource-constrained contexts.

The EU should consider working with key partners in the Global South to start discussions around a potential multilateral initiative on data protection allowing for wider dialogues on data transfer from one region to another, rather than simply relying on the very high data adequacy standards of the GDPR. As mentioned above, this would imply creating strong alignment with partners who have some shared understanding around human-centric digitalisation and are already pushing for multilateral discussions on data policy such as India, South Africa, Kenya, organisations like Smart Africa, the AU, regional economic communities (RECs) in Africa, etc. The EU is a strong believer in multilateralism and has been one of the main forces driving the Digital Compact at the UN, which it hopes will set a minimum shared approach to digital governance. Similarly, the EU is enthusiastically supporting UNESCO's initiative on Platform Regulation, which it hopes will play a role in developing standards globally in much the way that the Digital Services Act seeks to do within the EU. However, to date, there has not yet been a realistic multilateral initiative on data sharing, and the EU relies on its own data adequacy agreements with third countries. A multilateral approach would allow for a more level playing field and shared rules. It is unlikely that such an initiative could bring together the very opposing approaches of certain global powers, but it might begin to build a base for a new approach to data sharing between a wider range of countries that live up to a certain standard of data protection.

This suggests that the EU should emphasise a vision of data sovereignty that does not only uphold high standards, but that also focuses on data for public good (DPG) and building local data economies. This means that while the EU sets standards on regulating the digital space, it should also promote the implementation of digital public goods: open-source, interoperable digital solutions that can then be used in partner countries to build digital public infrastructure such as e-ID, payment systems, etc. ensuring that these are built with a human-centric approach in a way that benefits all citizens and their economies. There are already positive examples of European initiatives supporting data for public goods in partner countries including the German Ministry for Development (BMZ) supporting the FAIR Forward project, which makes AI training services available in three African languages including Swahili. Another initiative is GovStack, which uses open-source tools, sandbox for testing and communities of practices to build inclusive and safe digital public infrastructure (World Economic Forum 2022).

4. Working with other global and regional actors

Developing shared approaches to digital sovereignty - both with traditional partners, such as the other G7 members, as well as with emerging powers like India, and regional blocs such as the African Union, will be essential to the EU's geopolitical aims regarding digital governance. The EU has long struggled with accusations that EU actors preach to partner countries in the Global South, rather than truly treating them as partners. When it comes to digital governance, and to the question of digital sovereignty, the EU cannot afford to be seen as preaching its vision without consideration of the needs and visions of others. The rhetoric around the “Brussels Effect” and the externalisation of internal EU regulations risks doing just this and alienating potential allies by focusing too much on them replicating EU regulations. It also risks undermining the EU’s claims about supporting the digital sovereignty of others. Thus, while the EU’s experiences are certainly worth sharing with partners, this should be done in a way that shows mutual respect and that relies on a more sophisticated digital diplomacy vis-a-vis partners. Such an approach is beginning to emerge vis-a-vis certain partners, but should be extended to wider partnerships with the Global South.

Here we look briefly at EU-US collaboration in the Global South, and at relations with India and Africa - notably the African Union - in order to illustrate different kinds of partnerships with different kinds of actors. Yet, there are a wide range of other actors with which the EU might collaborate further with around building shared approaches to digital sovereignty, including notably other G7 partners, members of the Association of Southeast Asian Nations (ASEAN) and countries in Latin America and the Caribbean.

The United States

The EU’s relationship with the **United States** around technology has been a fraught one and continues to experience highs and lows. Despite many commonalities, the different approaches to both digital regulation and on industrial policy, including most notably on data protection, the Digital Markets Act and Digital Services Act, and the Inflation Reduction Act, mean that the approaches of the two blocs are rarely in harmony (See Karkare 2023 and Musoni 2023 in this report). This is intimately connected to the very different approaches that the two are taking on questions of digital sovereignty - the EU more explicitly, the US implicitly - and notably their different visions for their own leadership role internationally.

Yet despite many differences, the EU and US largely manage to enjoy a relationship of mutual respect, finding common cause where they do have clear shared interests, such as in the recent ITU elections in 2022, which saw the election of American candidate, Doreen Bogdan-Martin as Secretary-General and Lithuanian Tomas Lamanauskas as Deputy Secretary-General. They also developed the Trade and Technology Council (TTC) as a forum to discuss some of the most tense issues around regulating, developing and promoting technologies. **The focus at the TTC on joint investments in digital infrastructure projects in third countries also offers an interesting example of bilateral cooperation, and if expanded could also allow for scalable and impactful projects.** Already, the EU and the US have agreed to jointly support the Kenyan government in developing its 2022-2032 National Digital Masterplan, as well as contribute in expanding Jamaica’s connectivity (EC 2022). It could also offer a valuable example for wider cooperation under the G7’s Partnership for Global Infrastructure and Investment, announced in 2022.

India

Over the past years, the EU and **India** have been tightening their bilateral relationship, driven by the changing geopolitical environment and India’s growing ambition to balance competition over critical technology supply chains and a reduced reliance on China (Kranenburg and Okano-Heijmans 2023). The culmination of this was the 2020 India-EU summit and the announcement in February 2023 of the establishment of a Trade and Technology Council (TTC) (EC 2023a) in the coming months as an attempt to make the relationship more strategic. There is clearly political will to push the partnership forward - each hopes to access the other market to support their strategic autonomy. The EU also hopes to achieve greater alignment with India in debates on global internet governance. Despite a certain degree of convergence of data regulation as a result of India slowly moving to view privacy as a fundamental right, their contrasting views on data protection have limited the relationship.

India stands to be a strong partner for the EU as it aims to ensure its own autonomy and takes a differentiated approach to China, however, it is not clear whether India’s data protection bill is compatible with the EU’s GDPR

(Voelsen and Wagner 2022). This is in part because the Indian government has made very close links between data protection and national security issues as well as putting emphasis on protectionist policies to drive the growth of the domestic industry for self-reliance. Further, India has also been criticised for being ambivalent on digital governance at the multilateral level. The EU is taking positive steps in institutionalising its partnership with India, but it will have to strengthen consultation with India via sustained dialogue to align their positions before debates at multilateral fora. Stronger consultations can also help them align their domestic policies with the international dimension. Furthermore, in the face of these opposing views, the EU needs to make concessions to be able to leverage other areas of the digital partnership. In particular, the EU's focus on norms and the differentiated approach to China remain key concerns for India (idem. 2022).

As the EU focuses on building a more strategic, and long-term relationship with India, it will be important for the EU to look at their digital partnership holistically rather than through a solely normative lens, which will also be key for the EU to promote a mutually reinforced and shared technological sovereignty with its partners (ETGovernment 2023). For example, it should leverage India's growing digital economy sector and work together to curb the dominance of the US and China in the platform economy. **There are also opportunities to work together in promoting digital public goods (DPGs) and digital public infrastructure (DPI) on the international stage, given India's strengths in these areas and the EU's own ongoing experiences developing interoperable cross-border DPI.**

Africa with focus on The African Union

The EU partnership with the **African Union** on digital transformation is very new. The EU strongly integrated digital transformation in its 'Comprehensive Strategy with Africa' in 2020, and this focus was further strengthened by the EU-AU investment package under the EU €300 billion Global Gateway connectivity initiative. There is ample room for improving the partnership, which at the moment is focused on planning a series of digital infrastructure projects and building out the digital component of the EU's development cooperation with Africa, including providing technical support to various digital policy processes in the continent. Through the GIZ Datacipation project and the Team Europe Initiative on Data Governance in sub-Saharan Africa, the EU is supporting the development of the AU Data Policy Framework, which states that 'the AUC, member states, RECs, African institutions and international organisations shall cooperate to create capacity to enable African countries to self-manage their data, take advantage of data flows, and govern data appropriately' (AU 2022). The framework reflects the AU's ambitions to achieve greater digital sovereignty for its Member States by building a common data market that could fuel African innovation ecosystems. It also shows the ambition to participate in multilateral discussions on data governance with one unified voice. Therefore, strongly anchoring the concept of digital sovereignty into the EU's fundamental rights framework and bringing it in firmly in its digital partnerships could be a major step towards better digital partnership and coordination at multilateral fora. This should entail a real negotiation around what the term means for policymakers on each side and how this can actually be implemented in practice.

To make the partnership truly mutually beneficial, there are a few aspects that need to change. First, the debates on digital transformation have been characterised by a strong imbalance between the two sides, although at the bilateral level (for example, Kenya), the relationship is evolving fast from traditional development cooperation to economic cooperation, based on investment for hard and soft infrastructure to push the country's own digital positioning in the region (Sergejeff et al. 2023). In particular, a shortage of strong technical expertise on the AU side has allowed the EU to remain assertive in its negotiation with African counterparts, often failing to consult them on key initiatives (Domingo 2022). **The EU should refrain from such unilateralism in its relations with Africa, instead supporting capacity building and encouraging the AU to invest more in digital expertise.** Secondly, **as the EU works for more policy coherence between its domestic and external domains, it should make sure that there is space to harmonise with Africa's regulatory frameworks.** For example, considering how to bring in the EU sphere countries who are not data adequate or that are shifting away from its model (for example, Kenya). Thirdly, **the EU should follow through on the promise of Global Gateway in Africa, although this will be a gradual process over several**

years. As discussed by Musoni in this report, safe and secure digital infrastructure is an essential element of achieving a certain degree of digital sovereignty and ensuring data is secure. Thus, supporting a major uptick in EU investment in reliable digital infrastructure is a key element of showing real support to Africa's digital sovereignty, although this is not simply a question of new money now, but of a sizable increase in public and private investments over the coming years (Teevan 2023).

5. Conclusion and summary of recommendations

In this chapter, we have started to lay out certain elements that the EU would need to address in order to develop an approach to digital sovereignty that appeals at the international level, and can support EU digital partnerships with developing countries in the Global South. Firstly, we have argued that the EU will need to demonstrate how its policies support and do not hinder the digital sovereignty of partner countries, notably by demonstrating that its domestic policies are consistent with its international rhetoric on building stronger partnerships and alliances with countries in the Global South based on mutual respect and real dialogue. Secondly, we have argued that the EU will need to work with others to develop joint approaches to key concepts behind its vision of digital sovereignty, notably the notion of human-centric digital transformation if it hopes to truly make this a shared driver of policy discussions with partners and at multilateral fora. Thirdly, we argued that the EU should take a more flexible approach in its partnerships with third countries, including notably on data governance, so as to develop a wider range of partnerships and thus have greater influence. Finally, we briefly looked at how the EU might work with certain countries and regions to come up with a shared basic understanding of digital sovereignty. This shared understanding would seek to identify some common principles while acknowledging that there will be some divergences based on different levels of development and different national interests. This might in turn allow the EU to work with others to negotiate certain international rules and standards.

Below, we summarise some of the recommendations that were developed throughout this last chapter:

1. **Consistency between internal and external policies:**

- Integrate the external dimension into all domestic strategies, and carry out real impact assessments with regard to the impact of domestic regulations externally. The EU has adopted a host of measures to strengthen its own digital ecosystems through digital regulation and industrial policy. Yet, in order to truly live up to the ideals of the geopolitical commission and reflect the external dimension of these domestic policies, they should be backed up by more detailed studies looking at what the effects of these policies are for third countries, and particularly for developing countries in the Global South. An initial step might be to carry out a broad study looking at how the external dimension has been integrated to date, and what steps might be taken to strengthen the external dimension of existing policies.
- Develop plans for how the EU's growing focus on domestic industrial policy can also integrate partner countries' interests and ambitions, potentially integrating them into EU value chains through further Global Gateway flagships. The TEI on vaccine manufacturing is one good example of this, which will both strengthen European industry and African resilience in the face of future epidemics or pandemics. Similarly, efforts are underway to integrate North African countries into European plans around the development of green hydrogen. As mentioned above, the reference to supporting processing of materials in partner countries in the Critical Raw Materials Act also offers an important opportunity to support industry in partner countries, and for the EU to differentiate itself from China. Most importantly for digital industries perhaps will be support to the data economy, and to demonstrating how the data economy can work for developing countries. For example, the TEI on Data Governance in Sub-Saharan Africa will need to deliver on not just strengthening digital governance in partner countries, but on developing practical use cases in a range of industries that demonstrate the economic utility of strengthening digital governance. Given the low rate of

adoption of digital technologies in developing countries, the focus should be on increasing the demand for technologies as well as their supply.

- In line with the above, the EU should also scale up support to local technology hubs, and offer more funding for research and innovation partnerships with developing countries. For example, concerted efforts to include universities and research institutes from developing countries in Horizon Europe projects could play an important role in supporting more joint initiatives that address developing country needs.

2. A common understanding of 'human-centric' digital transformation

- The EU should strongly embed its human-centric approach to digital transformation in its digital partnerships, but most importantly in its advocacy at multilateral organisations with concrete definitions and benchmarks to measure its impact.
- The EU can lead discussions to develop a common understanding of the concept of 'human centric' digital transformation together with partner countries, rather than focusing only on sharing its own still sometimes vague terminology. Understanding some of its partners' bargaining process between economic needs and human rights will be essential as the EU promotes a 'human-centric' digital governance model, including emphasising the benefits of strong data protection.

3. Data sovereignty as data for public good

- Understand that a very strict approach to the adoption of its regulatory frameworks, such as GDPR, might go against its geopolitical ambitions to promote its vision of data sovereignty given its partner's diverse social values and economic realities. Adopting a more varied approach may ultimately serve the EU's interests better, including continuing to support partners in developing their own approach to regulating the use of data, integrating local priorities, needs and capacities, expanding initiatives such as the AU-EU Data Governance programme, and also pursuing a new approach at the multilateral level. While the EU should continue to promote high data protection standards, it should also be open to coupling this with more flexible approaches that can potentially enable it to expand its reach.
- Consider working with key partners through bilateral dialogues, including India, ASEAN countries, key Latin American and African countries, as well as multilateral dialogues with the AU, Smart Africa, ASEAN, and leading private sector actors in the Global South to start discussion around a potential multilateral initiative on data sharing, complementing the work that the EU is doing with the UN Tech Envoy on the Global Digital Compact. For instance, this might include expanding on the Africa-Europe Digital Regulators Partnership by working with the Network of African Data Protection Authorities (NADPA) to develop a holistic understanding of the priority needs for African data protection regulators and developing frameworks which align with these needs. This might also entail working with partners to ensure that there is a common approach to guide key partners on how data should be processed, shared or transferred, and encourage key partners to reflect these guiding principles throughout bilateral and multilateral agreements.
- Emphasise a vision of data sovereignty that does not only uphold high standards, but that also focuses on data for public goods (DPG) and building local data economies. This is a key aspect of the AU-EU Data Governance programme that will need to be further elaborated through the development of practical use cases that have wide relevance and interest for African citizens, businesses and governments.

4. Building partnerships with key partners on digital sovereignty

- US:
  - Given a joint interest in offering alternatives to a Chinese model of cyber sovereignty in the Global South, the EU and US should expand the focus on joint investments in third countries at the TTC. This could offer an interesting example of bilateral cooperation, potentially allowing for more scalable and impactful projects. They would also provide valuable examples for wider cooperation under the G7's Partnership for Global Infrastructure and Investment, announced in 2022.

- As the joint advocacy of the EU, US and other like-minded partners around the ITU elections in 2022 demonstrated, joining forces at multilateral fora can lead to positive outcomes. However, the fundamental differences in terms of the approaches to data sharing and data sovereignty ultimately weaken potential cooperation, and will need to be overcome in order to develop a truly effective joint approach at multilateral fora.

- India:
  - There are opportunities to work together in promoting digital public goods (DPGs) and digital public infrastructure (DPI) on the international stage, given India's strengths in these areas and the EU's own ongoing experiences developing interoperable cross-border DPI. ECDPM will be doing more work looking at what might be possible in this area over the coming months.

- Africa:
  - The EU should continue to work with the AU and its members to ensure the flow of data between Africa and Europe, and ultimately work towards the closer integration of their respective digital single markets as stated in the EU-Africa Global Gateway Investment Package. For this, we have argued that the EU could open negotiations with African countries on a potential Data Privacy Framework. This could be accompanied by a new TTC with key players such as the Network of African Data Protection Authorities (NADPA), while deepening its understanding of the continent's digital ecosystem needs and context.
  - Meeting the commitments made under the Global Gateway Initiative, including mobilising EUR 150 billion in investment for digital infrastructure for Africa, will be crucial for the credibility and relevance of the EU as a valued global digital partner. However, the implementation of the Global Gateway initiative will be a gradual process over several years, and in this sense the mid-term review of the NDICI programming will also be crucial to assess whether the EU's digital diplomacy efforts are helping achieve its goals and adjust partners' expectations in the process. Developing a genuinely new approach in the way the EU, member states and private sector actors work together will also be essential to developing Global Gateway into something that truly delivers in the medium to long-term, going above and beyond initial commitments (Teevan 2023). This may include putting in place new innovative joint financing mechanisms - something ECDPM will explore in future work.

References: Summary

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

Basu, A. 2021. Sovereignty in a 'Datafied' World. Issue Brief 501. October 2021. Observer Research Foundation.

Bosoer, L. 2022. Digital Sovereignty: Voices from Latin America. European University Institute (EUI).

Burrows, M. and Mueller-Kaler, J. 2021. India's quest for digital sovereignty. In: Smart Partnerships amid Great Power Competition: AI, China, and the Global Quest for Digital Sovereignty. Washington DC: Atlantic Council.

Chin, K. 2023. What is the Digital India Act? India's Newest Digital Law. UpGuard.

Creemers, R. 2020. China's Approach to Cyber Sovereignty. Berlin: Konrad-Adenauer-Stiftung.

Degezelle, W. with Yahmadi, H., Mackenzie, T., Fathy, N. and Kummer, M. 2022 (Stantec). The Open Internet as cornerstone of digitalisation. The Global Gateway Partnership Opportunities between the European Union and Africa. Brussels: European Union.

Murgia, M. and Gross, A. 2020. Inside China's controversial mission to reinvent the internet. London: Financial Times.

Pons, A. 2023. Digital Sovereignty: for a Schuman Data Plan. European issues policy paper n°652. Brussels: Foundation Robert Schuman.

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.

References: Chapter 2

Adeleke, F. 2021. Exploring policy trade-offs for data localisation in South Africa, Kenya and Nigeria. Policy Brief 09. Johannesburg: Mandela Institute, School of Law, University of The Witwatersrand.

Agarwal, R. 2023. Industrial policy and the growth strategy trilemma. International Monetary Fund (IMF).

Andreoni, A. and Avenyo, E. 2021. South Africa is failing to ride the digital revolution wave. What it needs to do. The Conversation Media Group Ltd.

Ang, Y.Y. 2016. How China Escaped the Poverty Trap. New York: Cornell University Press.

Arcesati, R. 2020. The Digital Silk Road is a development issue. Berlin: Mercator Institute for China Studies (Merics).

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

Banga, K. 2018. Digitalization and the future of industrialization in Africa. GlobalDev.

Banga, K. 2022. Digital Technologies and Product Upgrading in Global Value Chains: Empirical Evidence from Indian Manufacturing Firms. The European Journal of Development Research, p.p. 77–102.

Beyleveld, A. and Sucker, F. 2022. Cross-Border Data Flows in Africa: Policy Considerations for the Afcfta Protocol on Digital Trade. Abuja: Centre for the Study of the Economics of Africa (CSEA Africa).

Bianchi, P., Durán, C. R., and Labory, S. (Eds.). 2019. Transforming Industrial Policy for the Digital Age. Cheltenham: Edward Elgar Publishing.

Boones, L., Haas, J. Haugh, D. and Shin, Y-H. 2022. How can Europe catch up on its digital backlog. Ecoscope.

Bradford, A. 2020. The European Union in a globalised world: the "Brussels effect". pp. 75-79. Paris: Groupe d'études géopolitiques.

Breton, T. 2022. A European Sovereignty Fund for an industry "Made in Europe" LinkedIn.

Burrows, M. and Mueller-Kaler, J. 2021. Smart Partnerships amid Great Power Competition: AI, China, and the Global Quest for Digital Sovereignty. Atlantic Council.

Carrière-Swallow, Y., Haksar, V. and Patnam, M. 2021. Stacking up financial inclusion gains in India. Washington DC: International Monetary Fund.

Chang, H-J. 2001. Intellectual property rights and economic development - historical lessons and emerging issues. Penang: Third World Network.

Chaudhuri, R. 2021. Make in India and the PLI schemes will make India a manufacturing powerhouse: ET-ILC Members. The Economic Times. New Delhi: Times Internet Limited.

Chen, S. 2023. US sanctions boost China's R&D investment and output in some hi-tech fields: Chinese study. South China Morning Post.

Chivunga, M. and Tempest, A. 2022. Driving Digital Inclusion within the AfCFTA Framework. SAIIA Occasional Paper No. 338. The South African Institute of International Affairs.

Cobby, R. 2023. The Eurochip. New York: Phenomenal World.

Creemers, R. 2020. China's Approach to Cyber Sovereignty. Bonn: Konrad-Adenauer-Stiftung.

Creemers, R. 2023. China's Tech Rectification. New York: The Wire.

Cyrill, M. 2023. Surge in Smartphone Exports from India Show Incentive Schemes Work. India Briefing.

Demarais, A. 2022. How the U.S.-Chinese Technology War Is Changing the World. Washington DC: Foreign Policy (FP).

Desai, V., Klapper, L. and Natarajan, H. 2022. Does digitizing government payments increase financial access and usage? Washington DC: The Brookings Institution.

Detsch, C. 2023. Waking the sleeping beauty of European industrial policy. International Politics and Society.

De Ville, F. 2023. The Return of Industrial Policy in the European Union. Ghent: Ghent University.

Domingo, E. 2023. The achilles heel of Kenya's growing digital economy. ECDPM Commentary. Maastricht: ECDPM.

Domingo, E. and Tadesse Shiferaw, L. 2022a. Digitalisation and Democracy: Is the African Governance Charter fit for the digital era? ECDPM Discussion Paper 331. Maastricht: ECDPM.

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

Durand, C. and Winkler, D. 2018. Intellectual Monopoly in Global Value Chains. The New School for Social Research.

EC. N.d.-a. European industrial strategy. Brussels: European Commission.

EC. N.d.-b. A European Strategy for data. Brussels: European Commission.

EC. N.d.-c. A European approach to artificial intelligence. Brussels: European Commission.

EC. N.d.-d. The Digital Markets Act: ensuring fair and open digital markets. Brussels: European Commission.

EC. N.d.-e. European Chips Act. Brussels: European Commission.

EC. 2022. Proposal for a Council regulation amending Regulation (EU) 2021/2085 establishing the Joint Undertakings under Horizon Europe, as regards the Chips Joint Undertaking. Brussels: European Commission.

EC. 2023a. Critical Raw Materials: ensuring secure and sustainable supply chains for EU's green and digital future. Brussels: European Commission.

EC. 2023b. A Green Deal Industrial Plan for the Net-Zero Age. Brussels: European Commission.

EC. 2023b. EU-India: new Trade and Technology Council to lead on digital transformation, green technologies and trade. Brussels: European Commission.

Economic Times. 2022. India's 5G roll out cost to be highest among emerging nations at up to $75 billion: Ericsson-Analysys Mason study. Times Internet Limited (Times Center). Noida: India.

Ehl, D. 2022. Africa embraces Huawei tech despite security concerns. Deutsche Welle (DW).

EIB. 2019. Who is prepared for the new digital age? European Investment Bank.

EIU. 2023. India's manufacturing moment. The Economist Intelligence Unit Limited. The Economist Group.

El Aynaoui, K., Jaïdi, L. and Zaoui, A. 2022. Digitalise to Industrialise. Egypt, Morocco, Tunisia, and the Africa–Europe Partnership. In: Daniels, C. Erforth, B. and Teevan, C. (Eds.). Africa–Europe Cooperation and Digital Transformation. London: Routledge.

Engheim, E. 2021. Industrial Policy in Postwar Finland. Medium.

Espinoza, J. 2020. EU vs Big Tech: Brussels' bid to weaken the digital gatekeepers. London: Financial Times.

Espinoza, J. 2023. Europe's Big Tech trust buster. Podcast. London: The Financial Times.

Fernando, N. 2023. SL exploring ways to adopt India's cross-border digital payment systems to attract more of their tourists. Dailymirror.lk.

Foster, C. and Azmeh, S. 2019. Latecomer Economies and National Digital Policy: An Industrial Policy Perspective. The Journal of Development Studies, 56:7, 1247-1262.

Goldsmith, J. 2015. The Tricky Issue Of Severing US "Control" Over ICANN. Hoover Institution.

Gunter, J. and Legarda, H. 2022. The global struggle to respond to an emerging two-bloc world. Berlin: Mercator Institute for China Studies (Merics).

Haeck, P. 2023. The Dutch get ensnared in US-China chips fight. Politico.

Harris, L. 2023. White House Offers Climate Subsidies to Rich Allies. The American Prospect.

Herrero, A.G. 2021. What is Behind China's Dual Circulation Strategy. China Leadership Monitor (CLM).

Hersey, F. 2022. Sri Lanka to begin procuring digital ID equipment from India with Indian money. Toronto: BiometricUpdate.com.

Higgott, R. and Reich, S. 2022. The age of fuzzy bifurcation: Lessons from the pandemic and the Ukraine War. Global Policy published by Durham University and John Wiley & Sons Ltd.

Hobbes, C. (Ed). 2020. Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry. Berlin: European Council on Foreign Relations (ECFR).

Hong, Y. and Goodnight, G.T. 2019. How to think about cyber sovereignty: the case of China. Chinese Journal of Communication, 13:1, pp. 8-26. Taylor & Francis Online.

Huang, J. and Tsai, K.S. 2022. Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China. The China Journal 2022, 88: pp. 2-28. The University of Chicago Press.

Juhász, R., Lane, N., Oehlsen, E. and Pérez, V.C. 2023. Trends in Global Industrial Policy. Industrial Analytics Platform (UNIDO).

Kearns, J. and Mathew, A. 2022. How India's Central Bank Helped Spur a Digital Payments Boom. Washington DC: International Monetary Fund.

Kleibert, J. and Mann, L. 2020. Capturing Value amidst Constant Global Restructuring? Information-Technology-Enabled Services in India, the Philippines and Kenya. The European Journal of Development Research.

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

Komminoth, L. 2023. Chat GPT and the future of African AI. African Business.

Koyama, N., Totapally, S., Goyal, S., Sonderegger, P., Rao, P. and Gosselt, J. 2021. Kenya's Digital Economy: A People's Perspective Report 2021. Dalberg.

Kuo, M.A. 2022. 'Chip War': The China-US Competition for Critical Technology. The Diplomat.

Kwet, M. 2021. Digital colonialism: The evolution of US empire. Amsterdam: Transnational Institute.

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

Lema, R. and Rabellotti, R. 2023. The Green and Digital Transition in Manufacturing Global Value Chains in Latecomer Countries. Geneva: UNCTAD.

Leong, C.W.B. 2022. Chip War with Chris Miller. Analyse Asia.

Li, W., and Chen, Y. 2020. A Study of the Influence of Intellectual Property on China–U.S. Trade Relations. SAGE Open, 10(2).

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

Lu, S., Hao, K. and Huang, R. 2023. Why Chinese Apps Are the Favorites of Young Americans. New York: Wall Street Journal.

Luce, E. 2023. China is right about US containment. London: Financial Times.

Macdonald, A. 2022. Digital identity boosts public infrastructure for India, Philippines. Toronto: BiometricUpdate.com.

Mann, L. 2016. At the Intersection of Digital Economy and Industrial Policy in Africa. Blog. London: London School of Economics.

MAS. 2023. Launch of Real-time Payments between Singapore and India. Monetary Authority of Singapore.

Matthews, D. 2022. EU still behind on AI, but not as much as feared. Brussels: Science Business.

Mazzucato, M. 2013. The Entrepreneurial State: Debunking public vs. private sector myths. London: Penguin Books Ltd.

McGee, P. 2023. What it would take for Apple to disentangle itself from China. London: The Financial Times.

MeitY. 2018. CISOs Top Best Practices for a Safe & Secure Cyber Environment. Government of India, Ministry of Electronics & Information Technology (Cyber Security and Cyber Law Group).

Miller, C. 2019. A Semiconducted Trade War. Washington DC: Foreign Policy (FP).

Miller, C. 2022. Chip War: The Fight for the World's Most Critical Technology. Simon & Schuster.

Mims, C. 2022. Google, Amazon, Meta and Microsoft Weave a Fiber-Optic Web of Power. New York: Wall Street Journal.

Mirrlees, T. 2020. A US-China Rivalry? The Digital Technology and Cultural Industries. Global Dialogue.

Mitter, S. 2023. India has 115 unicorns with a cumulative valuation of over $350 billion. Business Today: The India Today Group.

Moss, T. 2023. Collateral damage from America's myopic mercantilism. Eat More Elections by Todd Moss.

Munga, J. and Denwood, K. 2022. How Will U.S.-China Tech Decoupling Affect Africa's Mobile Phone Market? Washington DC: Carnegie.

Musoni, M. 2023. Unpacking digital sovereignty through data governance by Melody Musoni. Chapter in: Global approaches to digital sovereignty: Competing definitions and contrasting policy approaches. Maastricht: ECDPM.

Nyabiage, J. 2022. US takes China rivalry over African influence underwater, with high-speed internet cable spanning continents. South China Morning Post.

Nymalm, N. 2019. Washington's old 'Japan problem' and the current 'China threat'. East Asia Forum.

Ogunjuyigbe, O. 2023. Meta's legal battles in Africa are rising. Ventures Africa.

Orufa, S. 2023. African startups working to expand internet access across the continent. Ventures Africa.

Pannier, A. (Ed.) 2023. The Technology Policies of Digital Middle Powers. Paris: Institut français des relations internationales (IFRI).

Pant, H.V. and Tirkey, A. 2021. India Draws a Line in the 5G Sand. Washington DC: Foreign Policy (FP).

Phartiyal, S. 2023. India May Share Tech With African Nations for Digital Pay Systems, Public Health Apps. Bloomberg.

Posen, A. 2023. America's Zero-Sum Economics Doesn't Add Up. Washington DC: Foreign Policy (FP).

Rathenau Instituut. 2022. China: a scientific superpower in the making. Den Haag: Rathenau Instituut.

Rudd, K. 2022. The World According to Xi Jinping: What China's Ideologue in Chief Really Believes. Foreign Affairs.

Said, J. 2021. It is time to switch on the transformative power of industrial policy in Africa. The Pan African Review.

Sampath, P.G. and Tregenna, F. (Eds.). 2022. Digital Sovereignty: African Perspectives. Johannesburg: DSI/NRF South African Research Chair in Industrial Development.

Saran, S. 2016. Navigating the Digital 'Trilemma'. New Delhi: Observer Research Foundation (ORF).

Shen, X. 2021. China's crackdown on Big Tech is a short-term cost for long-term health: state media. South China Morning Post.

Solon, O. 2017. 'It's digital colonialism': how Facebook's free internet service has failed its users. The Guardian.

Stolton, S. and Haeck, P. 2023. Europe embarks on subsidy race it can't win. Politico.

Swaniker, F. 2023. The secret to creating millions of technology jobs in Africa. LinkedIn.

Teevan, C. 2023. Building a digital single market: From the EU to Africa. ECDPM Briefing Note 155. Maastricht: ECDPM.

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

Teleanu, S. 2021. The geopolitics of digital standards: China's role in standard-setting organisations. DiploFoundation/Geneva Internet Platform and Multilateral Dialogue Konrad Adenauer Foundation Geneva.

The Economist. 2022. Can China create a world-beating AI industry? The Economist Group.

The Economist. 2023a. America's commercial sanctions on China could get much worse. The Economist Group.

The Economist. 2023b. India is getting an eye-wateringly big transport upgrade. The Economist Group.

The Economist. 2023c. Are Western companies becoming less global? The Economist Group.

Thibaut, K. 2022. Chinese discourse power: Ambitions and reality in the digital domain. Washington DC: Atlantic Council.

Timmers, P. 2022. Digital industrial policy for Europe. Report. Centre on Regulation in Europe (CERRE).

Tooze, A. 2023. Chartbook #198 Globalization: The shifting patchwork. Adam Tooze.

UNCTAD. 2020. Technology and innovation report 2021: Catching technological waves. Innovation with equity. New York: United Nations Publications.

UNIDO. 2019. Industrial Development Report 2020. Industrializing in the digital age. Vienna: United Nations Industrial Development Organization.

von der Leyen, U. 2023. Speech by President von der Leyen on EU-China relations to the Mercator Institute for China Studies and the European Policy Centre. Brussels: European Commission.

Werner, J. 2018. China Is Cheating at a Rigged Game. New York: Foreign Policy (FP).

Wolf, M. 2023. The EU's future in a world of deep disorder. London: Financial Times.

Wübbeke, J., Meissner, M., Zenglein., M.J., Ives, J. and Conrad, B. 2016. Made in China 2025: The making of a high-tech superpower and consequences for industrial countries. Berlin: Mercator Institute for China Studies (Merics).

Yang, Y., Hancock, A. and Pitel, L. 2023. Solar power: Europe attempts to get out of China's shadow. London: Financial Times.

Zhang, S.Y. 2021. Using equity market reactions and network analysis to infer global supply chain interdependencies in the context of COVID-19. Journal of Economics and Business, Volume 115. Science Direct.

References: Chapter 3

Amnesty International. 2022. 1. “Community of common destiny” or “community of shared future”. Amnesty International.

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

Bauer, M. 2020. Europe’s Quest for Technology Sovereignty: Opportunities and Pitfalls. Brussels: European Centre for International Political Economy (ECIPE).

Broeders, D., Cristiano, F. and Kaminska, M. In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions. Journal of Common Market Studies (JCMS).

Burwell, F. and Propp, K. 2022. Digital sovereignty in practice: The EU’s push to shape the new global economy. Washington DC: Atlantic Council.

CoEU. 2022. Council Conclusions on EU Digital Diplomacy. Brussels: Council of the European Union.

CONCORD. 2023. Demystifying the people-centred approach for the digital transformation. Brussels: CONCORD.

Domingo, E. 2022. Bringing African digital interests into the spotlight. ECDPM commentary. Maastricht: ECDPM.

EC. 2020a. Impact assessment of the Digital Services Act. Brussels: European Commission.

EC. 2020b. Joint Statement - 15th EU-India Summit, 15 July 2020. Brussels: European Council and Council of the European Union.

EC. 2021a. Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions. 2030 Digital Compass: the European way for the Digital Decade. Brussels: European Commission.

EC. 2021b. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank. The Global Gateway. Brussels: European Commission.

EC. 2022. EU-US Joint Statement of the Trade and Technology Council. Brussels: European Commission.

EC. 2023a. Critical Raw Materials: ensuring secure and sustainable supply chains for EU's green and digital future. Brussels: European Commission.

EC. 2023b. EU-India: new Trade and Technology Council to lead on digital transformation, green technologies and trade. Brussels: European Commission.

EEAS. 2016. Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union’s Foreign And Security Policy. Brussels: European External Action Service.

EEAS. 2022. US/Digital: EU opens new Office in San Francisco to reinforce its Digital Diplomacy. European External Action Service.

ETGovernment. 2023. EU signs tech tie-up with India, to set up Trade & Technology Council for deeper cooperation in digital governance. ETGovernment.

EUCO. 2020. Special meeting of the European Council (1 and 2 October 2020): Conclusions. Brussels: European Council.

Kranenburg, V. and Okano-Heijmans, M. (Eds). 2023. How strategic tech cooperation can reinvigorate relations between the EU and India. Clingendael Report. The Hague: Clingendael.

Mannion, C. 2020. Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets. Vol. 53. Vanderbilt Law Review.

Pisa, M. and Nwankwo, U. 2021. Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development. Washington DC: Center for Global Development.

Pons, A. 2023. Digital Sovereignty: for a Schuman Data Plan. European Issue n°652. Fondation Robert Schuman.

Rimbaud, E. 2021. Le peuple souverain et l'espace numérique. Paris: Le Grand Continent.

Sergejeff, K., Domingo, E. and Veron, P. 2023. The EU, geopolitics and human development: Insights from Zambia, Kenya and Guinea. ECDPM Discussion Paper 340. Maastricht: ECDPM.

Teevan, C. 2019. Geopolitics for dummies: Big challenges await the new European Commission. ECDPM Commentary. Maastricht: ECDPM.

Teevan, C. 2023. Global Gateway as new approach, not simple funding pot. EURACTIV.

Teevan, C. and Sherriff, A. 2019. Mission possible? The Geopolitical Commission and the partnership with Africa. ECDPM Briefing Note 113. Maastricht: ECDPM.

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

United Nations. 2021. Leave No One Behind: A People-Centered Approach to Achieve Meaningful Connectivity. United Nations.

Vestager, M. 2022. Speech by Executive Vice-President Vestager on the Declaration on Digital Rights and Principles. Brussels: European Commission.

Voelsen, D. and Wagner, C. 2022. India as an Ambivalent Partner in Global Digital Policy. Potential and Limits of Cooperation in the Digital Economy and Internet Governance. Stiftung Wissenschaft und Politik (SWP).

World Economic Forum. 2022. Inclusive digital infrastructure can help achieve the SDGs. Here's how. World Economic Forum.

About ECDPM

ECDPM is an independent 'think and do tank' working on international cooperation and development policy in Europe and Africa.

Since 1986 our staff members provide research and analysis, advice and practical support to policymakers and practitioners across Europe and Africa – to make policies work for sustainable and inclusive global development.

Our main areas of work include:

- EU foreign and development policy
- Migration and mobility
- Digital economy and governance
- AU-EU relations
- Peace, security and resilience
- Democratic governance
- Economic recovery and transformation
- Climate change and green transition
- African economic integration
- Sustainable food systems

For more information please visit www.ecdpm.org

This publication benefits from the structural support by ECDPM's institutional partners: Austria, Belgium, Denmark, Estonia, Finland, Ireland, Luxembourg, The Netherlands and Sweden.

ISSN1571-7577

Funded by
the European Union

ecdpm

HEAD OFFICE
SIÈGE
Onze Lieve Vrouweplein 21
6211 HE Maastricht
The Netherlands *Pays Bas*
Tel +31 (0)433 502 900

BRUSSELS OFFICE
BUREAU DE BRUXELLES
Avenue des Arts 44, 1000
Brussels *Bruxelles*
Belgium *Belgique*
Tel +32 (0)28 825 008

info@ecdpm.org
www.ecdpm.org
KvK 41077447