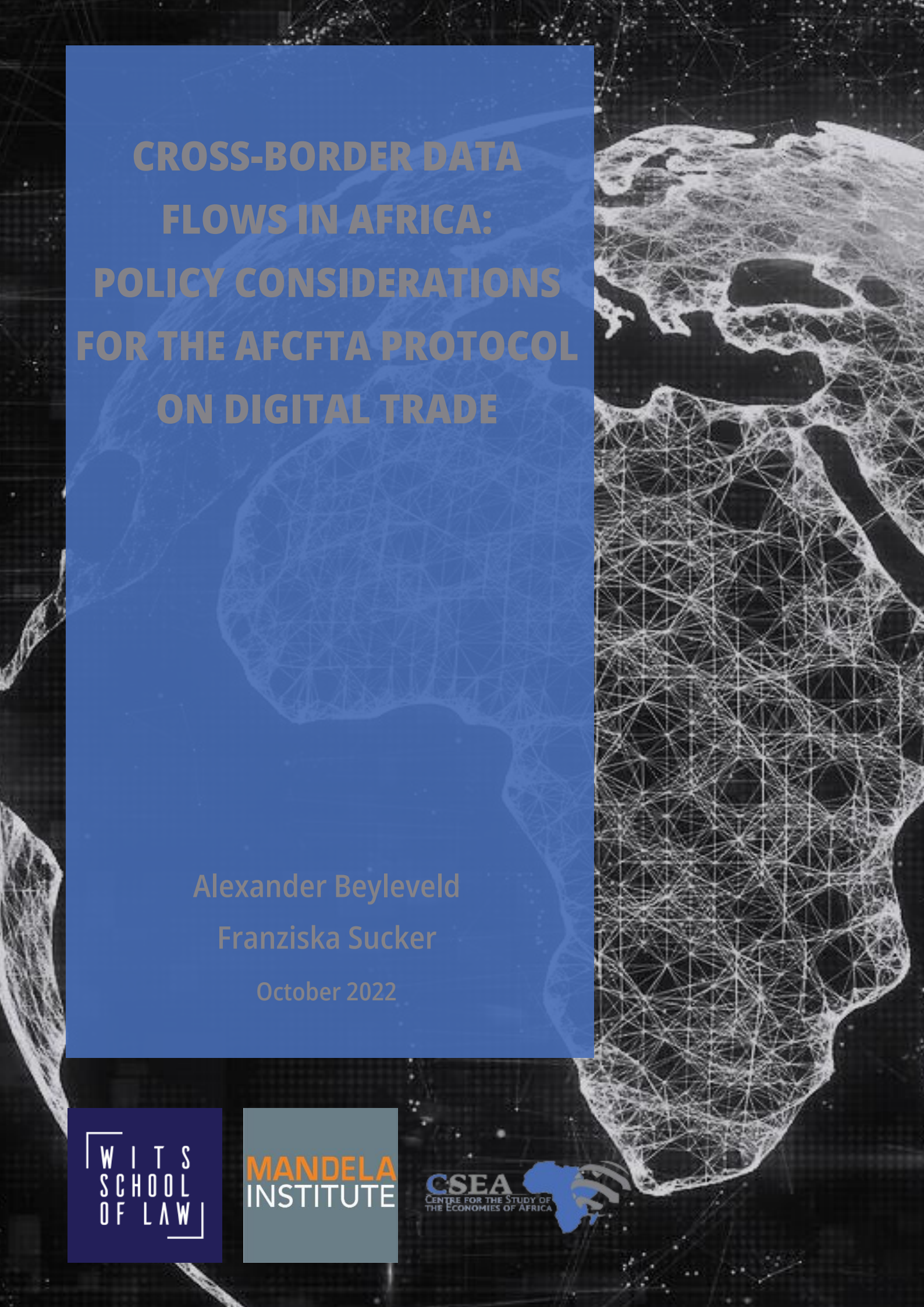

CROSS-BORDER DATA FLOWS IN AFRICA: POLICY CONSIDERATIONS FOR THE AFCFTA PROTOCOL ON DIGITAL TRADE

Alexander Beyleveld

Franziska Sucker

October 2022

WITS SCHOOL OF LAW

MANDELA INSTITUTE

CSEA CENTRE FOR THE STUDY OF THE ECONOMIES OF AFRICA

This page is left intentionally blank.

CONTENTS PAGE

1 Introduction and motivation*

The original Industrial Revolution was powered by steam; the second by electricity. The rise of digitisation and automation generally defined the Third Industrial Revolution, which was largely powered by oil. Today, we find ourselves in the Fourth Industrial Revolution (4IR), which is largely powered and characterised by data. It can hardly be contested that data is central to today's global economy in ways which it never has been before. Data flows across borders far more frequently than at any other point in time. Most importantly, these flows are creating or have created immense value (at least on aggregate) and are, therefore, central to businesses and business practices. They have fundamentally changed what and how much is traded, as well as with whom and how trade is conducted. Put differently, cross-border data flows have increased the scope, scale, and speed of trade.

Many models of the digital and data economies emphasise that data are generally generated as a by-product of economic activity, collected, processed for prediction purposes, and ultimately used to reduce uncertainty, which in turn increases the profitability of firms.[1] Moreover, data, particularly big data, is also an essential input for many new products and services in the digital world, including those which rely on so-called artificial intelligence (AI). As such, data powers the digital and data economies much in the way that oil or electricity fuels the non-digital economy. However, two particular characteristics of data make it a driver of the global economy different from those that have come before. The first key difference is that data, in digital form,[2] are, at least in principle, non-rivalrous, i.e., they can be consumed by one person without reducing the amount

* The scope of this report does not allow for us to make recommendations which are exhaustive or as comprehensive as we would like. The same applies to most discussions on conceptual issues, and on benefits and costs of specific regulatory interventions. They are neither exhaustive nor comprehensive.

[1] See, for example, Maryam Farboodi and Laura Veldkamp, 'A Model of the Data Economy' (Columbia Business School Working Paper 2021) <https://bit.ly/3JpIRt9> accessed 10 April 2022.

[2] On the meaning of 'data' and its various types, see section 2.1 below.

or quality available to others.[3] As a result, data are also replicable at essentially zero cost – the second difference.

Like the three eras that preceded it, the 4IR has brought with it significant changes in the ways in which value is created in the contemporary global economy, opening up opportunities and new possibilities. It has also brought about rapid changes to the fabric of our societies. More precisely, like the industrial revolutions that preceded it, the 4IR has led to social upheaval of significant proportions as people react to the changes around them. Today, those who have managed to leverage data to their advantage are, in material terms at least, wealthier than any others in human history. At the same time, as the pace of technological change has ramped up, others have fallen further behind than they already were at the start of the 4IR, rendering their jobs nugatory or placing pressure on their incomes because their work functions have become threatened by machines and algorithms. It is thus unsurprising that economic inequality continues to soar within our societies, particularly as the disruptions stemming from the COVID-19 pandemic intensified the adoption of technologies and the pre-existing advantages of those best able to exploit them.

Additionally, as countries have scrambled to get to the technological frontier, geopolitics, too, has shifted. The economic rise, particularly of China, means that we no longer live in a world dominated by one hegemonic actor. As a result, we are once again faced with a situation whereby the world's most powerful countries (or blocs of countries), while still significantly interdependent, are vying for economic supremacy, but are doing so largely distinctly from previous ways. Countries' response to non-consensus, and resultant global – multilateral – economic governance being stuck, has, among others, led to the rise of regionalism because smaller blocs of countries have sought to regulate contemporary issues with others who are of a similar mind and approach.

[3] See, for example, Avi Goldfarb and Catherine Tucker, 'Digital Economics' (2019) 57 Journal of Economic Literature 3, 12 (who argue that the extent to which -non-rivalry really exists in practice, is a function of legal and/or technological efforts to exclude). See also Charles I Jones and Christopher Tonetti, 'Nonrivalry and the Economics of Data' (2020) 110 American Economic Review 2819.

Hence, the regulation of issues arising from contemporary technological change, particularly the shift to an economy which is data-centric, has been rather slow and highly fragmented.

Against this backdrop, the regulation of cross-border data flows has come to the fore fairly recently possibly impacting international trade, economic development and other non-economic issues such as protecting the privacy of the individuals who interact within the digital and data economies. In the African context, negotiations on an African Continental Free Trade Area (AfCFTA) Digital Trade Protocol, i.e., within the AfCFTA framework for establishing a single market on the African continent, are currently underway. Given the fact that cross-border data flows may very well be regulated by this Protocol once concluded, the overarching aim of this report is to contemplate the various issues at stake in this regard and to provide policy recommendations on how to approach the regulation of cross-border data flows at the continental level. We undertake this exercise cognisant of the developments alluded to above, but from the perspective of African countries and the particular challenges they face, including the creation of a continental digital market among countries that have not yet all fully assimilated to the digital economy in ways which facilitate their economic growth.

We begin by clarifying the terminology used in the report (in section 2) with a view to fostering a shared understanding of the substance of a number of concepts relevant for purposes of a proper discussion of cross-border data flow regulation in an international trade context. We then turn to examine existing approaches towards the regulation of cross-border data flows from the perspective of adopting trade distortive data flow restrictions vis-à-vis allowing its free flow (in section 3). We do so from the vantage point of (i) national / supranational laws and regulations (in section 3.1) and (ii) international / regional laws and regulations (in section 3.2). We do this with the dual aim of (i) documenting the status quo insofar as regulatory approaches to cross-border data flows are concerned in some of the more powerful economic jurisdictions in the world, namely the United States (US), European Union (EU) and China, as well as in African countries (with a particular focus, at the national level, on Kenya, Nigeria and South Africa), and (ii) potentially drawing lessons from existing experience for regulating cross-border data flows in the AfCFTA context. To further inform our policy recommendations for AfCFTA State Parties to consider when

negotiating potential rules on cross-border data flows, we turn to discuss some of the main regulatory, institutional, and other challenges that arise in relation to regulating cross-border data flows (in section 4). We conclude by providing policy recommendations that may assist African countries with navigating the peculiarities of the continent and that aim to ensure they are able to fully tap the economic potential of increasing cross-border data flows (in section 5).

2 Terminology

Due to the constantly evolving, overlapping and frequently contested nature of definitions used when discussing cross-border data flows, the terminology we employ in this report requires clarification. Clarification matters because a common understanding of terms and concepts is central for, among other things, setting policy objectives and providing guidance for rulemaking, adjudicating rules, and regulation more broadly.

'Cross-border data flows' refers to the movement or transfer of data between servers across the borders of (mostly) countries, i.e., from within the boundaries of one geographic unit to another, via networking equipment that enables such transmission. Generally, data flows across borders when individuals, firms or governments authorise data to be transferred from one country (the source of the data) to another country where the data may be processed or used in other ways.[4] Once data has crossed a border, actors in the country of origin may lose what control they initially had over the data. This definition requires clarifying various related terminology. Most importantly, we must clarify what 'data' means (section 2.1). Other relevant terms used when discussing the regulation of cross-border data flows, which we define below, include 'data protection' and 'data subjects' (section 2.2), 'data localisation' (section 2.3), 'cybersecurity' (section

[4] See United States International Trade Commission, 'Digital Trade in the U.S. and Global Economies, Part 1' (USITC Publication 4415, Investigation No 332-531, 2013) <https://usitc.gov/publications/332/pub4415.pdf> accessed 18 September 2022; United States International Trade Commission, 'Digital Trade in the U.S. and Global Economies, Part 2' (USITC Publication 4485, Investigation Number: 332-540, 2014) <https://www.usitc.gov/publications/332/pub4485.pdf> accessed 18 September 2022; Jessica R Nicholson and Ryan Noonan, 'Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services' (US Department of Commerce, Economics and Statistics Administration, ESA Issue Brief 01-14,) <https://bit.ly/3QTJAH1> accessed 18 September 2022.

2.4), 'digital trade' (section 2.5), as well as terms such as 'data protectionism', 'barriers to digital trade' and 'restrictions to cross-border data flows which distort trade' (section 2.6).[5]

2.1 Data

While the term 'data' has a general meaning (see section 2.1.1), the concept has many facets and consists of many types at varying levels of granularity (see section 2.1.2). Therefore, we need to be precise when talking about data. It is only with an understanding of what exactly a particular author, policymaker or legislator has in mind when using the term 'data' in a particular context that one can meaningfully comprehend how the data economy operates, whom it benefits and why, and how to regulate certain issues to pursue specific objectives.

2.1.1 General meaning of 'data': count noun versus mass noun

According to the Oxford English Dictionary (OED), one finds that the word 'data' may refer to a *count* or mass (i.e., *non-countable*) noun. In the first context, 'data' is the plural form of the word 'datum', which is defined as 'an item of information'.[6] In the second context (i.e., as *mass* noun), 'data' refers to information being considered collectively, i.e., as what is frequently referred to as a 'set'. Such information is usually obtained by scientific work or exists as the result of computer processing. More specifically, for the OED, '[r]elated items of (chiefly numerical) information considered collectively, [are] typically obtained by scientific work and used for reference, analysis, or calculation', with each different item or piece of source information constituting a separate countable element.[7] Additionally, the OED defines data in a specific *computing* sense, where the word refers to collectively considered operations on '[q]uantities, characters, or symbols … [, which] are performed by a computer'. In the latter *computing* sense, 'data' might also refer to 'information in digital form', at least in non-technical contexts.[8] In a technical context, 'data' is

[5] While there are many other definitions that may be of relevance, those identified here are sufficient for the purpose of this report.
[6] See definition 1 of the entry 'data, *n.*' in Oxford English Dictionary (OED) online.
[7] See definition 2.a of the entry 'data, *n.*' in Oxford English Dictionary (OED) online.
[8] See definition 2.b of the entry 'data, *n.*' in Oxford English Dictionary (OED) online.

sometime contrasted with the word 'information',[9] with the distinction being that data are 'unprocessed facts or details, whereas information is processed, organised, or structured data',[10] i.e., 'data' becomes 'information' when it has been transformed in one way or another to make the collection – the 'raw' data – more useful or user-friendly to whomever (or whatever) is working with it for a given purpose.

What this discussion begins to illustrate is that, when speaking about 'data', whether the intended meaning is technical or non-technical, if we are not specific with our words or if we proceed without due reference to the context in which the term is being deployed, there is much room for confusion. As we will see below, the room for misunderstandings or talking past one another only increase as we begin to get more granular and technical with respect to our definitions.

2.1.2 Distinguishing between different types of data

Against the backdrop of these general definitions, various types of data can be distinguished, virtually all of which are capable of transmission across borders, which are, in practice, constructed through discourse and laws. Some of these can be viewed as sub-definitions of the count or mass noun definitions discussed above. They relate to specific ways in which the term 'data' is conceived of and are dependent on the specific context in which the term is used. Sometimes there is a focus on the amounts of data, for example, when we speak of 'big data' (discussed in section 2.1.2.1). Other times, the focus lies elsewhere, including on: the manner of its transmission, for example when 'electronic data (e-data)' or 'digital data' are being referred to (discussed in section 2.1.2.2); its accessibility, for example when contemplating the notion of 'open data' (discussed in section 2.1.2.3); its purpose, for example when considering whether data is 'public intent data' or 'private intent data' (discussed in section 2.1.2.4); and its nature or to whom it pertains, for example in the context of trying to determine whether given data is 'personal' (discussed in section 2.1.2.5).

[9] See definition 2.b of the entry 'data, *n.*' in Oxford English Dictionary (OED) online.
[10] See Susan Ariel Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (2019) 18 World Trade Review 541, 541–542.

Without claiming the following discussion to be exhaustive, we explain some of the most prominent constructions to illustrate the ways in which the term may be used, while acknowledging that other legal and non-legal constructions are used in the context of data, including by referring to terms such as 'confidential data', 'critical data', 'geolocation data', 'consumer data', 'biometric data' and 'classified data', to mention a few.

2.1.2.1 Big data

Due to the '[t]he hype about data economics [that] has arisen because of breakthrough data technologies, like machine learning and artificial intelligence', which consist of algorithms used for prediction,[11] it is data in the mass noun context that has become of interest to economists in recent years. Algorithms 'require enormous amounts of data, which are naturally generated by transactions: information about online buyers, satellite images of traffic patterns near stores, textual analysis of user reviews, click through data, and other evidence of economic activity'.[12] Some of these data sets that are too large or complex to be dealt with by traditional data processing application software. However, most definitions of 'big data', which is itself a contested term, go beyond mere large datasets.[13] More specifically, in the contemporary economics literature it usually refers to data which is

> huge in *volume*, consisting of terabytes or petabytes of data; high in *velocity*, being created in or near real time; diverse in *variety*, being structured and unstructured in nature; *exhaustive* in scope, striving to capture entire populations or systems; fine-grained in *resolution*, aiming to be as detailed as possible, and uniquely *indexical* in identification; *relational* in nature, containing common fields that enable the conjoining of different data

[11] Farboodi and Veldkamp (n 1) 2.
[12] Farboodi and Veldkamp (n 1) 2.
[13] Some sources do seemingly still define 'big data' primarily by virtue of its size. For example, one definition holds that 'big data' is '[a] term used to describe large data files that are embedded in the Internet and which can often be accessed easily by users; for example, census data'. See the entry on 'big data' in Darrel Ince (ed), *A Dictionary of the Internet* (4th edn, Oxford University Press 2019). Kitchin seems to disagree that census data is necessarily 'big data': see Rob Kitchin, 'Big Data, New Epistemologies and Paradigm Shifts' (2014) 1 Big Data & Society 205395171452848, 2.

> sets[;] and *flexible*, holding the traits of extensionality (can add new fields easily) and scalability (can expand in size rapidly).[14]

Moreover, '[t]he predictions made with this big data are typically used for business process optimization, such as advertising, forecasting sales, earnings, inventories, shipping needs or the future value of firms and their product lines'.[15] According to Farboodi and Veldkamp, 'this is where the *technological change* took place'.[16] They, therefore, assert that when we speak of data in regulatory contexts, it is actually big data with which regulators are concerned.[17]

2.1.2.2 Digital data / electronic data (e-data)

To further complicate matters, data often gets equated with the manner of its transmission. Computer networking, the set of ideas that gave us the internet, operates on the idea of information (in the non-technical sense) being captured in digital (usually binary) format. Loosely speaking, this enables information to be *carried* or *transmitted*, via some form of transmission medium like an electromagnetic wave, from one place to another using discrete (as opposed to continuous) signals. In a more specific sense, though, there is a distinction to be drawn between that information and the transmission medium used to move it from one place to another. If a fibre-optic cable is used, for example, then the transmission medium is light waves. But the information (or data in certain senses), which the light waves help to transmit, exists in the abstract, and it exists separately from its physical embodiment. This physical embodiment is often thought of as data. In this sense, data is a sequence of waves which conveys an ordered set of ones and zeroes to the recipient, that is, the waves pass binary codes from one place to another. Once the binary codes are received, they can be stored, developed, further transmitted or distributed,

[14] See Rob Kitchin, 'Big Data and Human Geography: Opportunities, Challenges and Risks' (2013) 3 Dialogues in Human Geography 262, 262. See also Kitchin (n 14) 1–2.; Farboodi and Veldkamp (n 1); Goldfarb and Tucker (n 3).
[15] Farboodi and Veldkamp (n 1) 2.
[16] Farboodi and Veldkamp (n 1) 2. Emphasis added. Farboodi and Veldkamp accredit this insight to Goldfarb and Tucker (n 3).
[17] Farboodi and Veldkamp (n 1) 2. Emphasis added. Farboodi and Veldkamp accredit this insight to Goldfarb and Tucker (n 3).

interpreted for a particular use or immediately executed using various forms of information technology.

To make this more concrete, let us consider an example. If we write a list of names and phone numbers on a piece of paper, the information we have written down – not the piece of paper with ink on it – can be thought of as data; let us call this type one data. The information on the piece of paper can then be coded into a sequence of ones and zeroes, for example using word processing software, and stored digitally – but still physically – on a hard drive. This physical embodiment can then be converted into a set of light waves (a different physical embodiment), which can be transmitted somewhere else. We can think of either of these two physical embodiments as data; let us call them type two data. Type one and two data differ as follows: type one in this example is the information in the abstract, the names and phone numbers, whereas type two is the physical embodiment of those names and phone numbers, which exists in one way or another as binary codes. To clarify this distinction when speaking of the different types, we refer to type one data simply as 'data' and to type two data as 'digital data' or 'electronic data (e-data)'.

2.1.2.3 Open data

Another example of a construction of a data type is the notion of 'open data', which, in a general sense, entails data which 'is free to use, re-use or redistribute … subject at most to measures that preserve provenance and openness'.[18] Conceived this way, i.e. with a focus on its accessibility, 'open data' may consist of two dimensions: first, the data must be 'legally open', which means 'they must be placed in the public domain or under liberal terms of use with minimal restrictions';[19] and, second, the data 'must be technically open, which means they must be published in electronic formats that are machine readable and non-proprietary, so that anyone can access and use the data using common, freely available software tools'.[20] While this definition stems from the World

[18] See World Bank, *Open Data Toolkit*, 'Open Data Defined' in 'Open Data Essentials' <http://opendatatoolkit.worldbank.org/en/essentials.html> accessed 18 September 2022.
[19] See World Bank (n 18).
[20] See World Bank (n 18).

Bank's Open Data Toolkit,[21] similar definitions can be found in legal or policy instruments at various levels of governance. For example, the City of Cape Town in South Africa has, in its Open Data Policy of 2020, defined 'open data' as 'data that can be freely used, shared and built-on by anyone, anywhere, for any purpose'.[22]

2.1.2.4 Public / private intent data

Other constructions of 'data' do rely on the purpose for which it was collected. For example, to illustrate some of the different ways in which data can be of value, the World Bank, in its 2021 World Development Report, distinguishes between 'public intent data' and 'private intent data'.[23] 'Public intent data' relates to data originally collected for public purposes, such as census data, national account data or public procurement data. 'Private intent data' refers to data collected for commercial purposes, such as administrative data from company financial accounts, or data on choices from digital platforms in the private sector.[24] This is not a legal construction, but rather a conceptual one for the purposes of developing a typology specific to this report to illustrate the different value of both types of data.[25]

2.1.2.5 Personal / non-personal data

In both economic and legal senses, an important distinction can be drawn between data that are 'personal' (discussed in section 2.1.2.5.1) and data that are not (discussed in section 2.1.2.5.2). It is also possible to have datasets which consist of both personal and non-personal data. These are commonly referred to as 'mixed datasets' (discussed in section 2.1.2.5.3). Notably, all the

[21] According to the World Bank itself, the 'Open Government Data Toolkit is designed to help governments, Bank staff and users understand the basic precepts of Open Data, then get "up to speed" in planning and implementing an open government data program, while avoiding common pitfalls'. See World Bank, *Open Data Toolkit* <http://opendatatoolkit.worldbank.org/en/index.html> accessed 18 September 2022.

[22] City of Cape Town Open Data Policy (Policy 27781) <https://bit.ly/3RSUo9H> accessed 18 September 2022.

[23] See World Bank, 'World Development Report 2021: Data for Better Lives' (World Bank 2021) 27–8.

[24] See World Bank (n 24) 27–8.

[25] Here, too, significant conceptual battles could be waged on the distinction between public and private intent and the extent to which this distinction should even exist. While it is not necessary for us to engage in these debates for present purposes, readers would do well to note that fault lines do exist and that a comprehensive data regulatory regime would need to either resolve these tensions or at the very least allow for them to be managed productively.

definitional caveats discussed above, i.e., the specific ways in which the term 'data' is conceived of, apply to personal, non-personal and mixed data sets.

2.1.2.5.1 Personal data

From a legal perspective, 'personal data' is most frequently defined in national legislation, but also in supranational legislation and sub-national legislation, as well as in free trade agreements (FTAs) and other international agreements, for example the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). While these definitions naturally vary from instrument to instrument, as a general proposition, 'personal data' refers to 'information relating to an identified or identifiable natural person'. This, for example, is how the term is defined in the KDPA.[26] The European Union's General Data Protection Regulation (GDPR) contains the exact same phrase as the KDPA, and adds that

> an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[27]

The Malabo Convention almost directly mirrors the GDPR definition. In Article 1, 'personal data' is defined as 'any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity'.

In several instruments the phrase 'personal information' is used, which entails the same or a similar definition. In section 1 of the South African Protection of Personal Information Act of 2013 (POPIA), for example, 'personal information' is defined, in part, as 'information relating to an identifiable, living, natural person'. This definition is even extended, 'where it is applicable', to 'an identifiable, existing juristic person'.[28] Section 1 of the POPIA then proceeds, much like Article 4(1)

[26] See KDPA, section 2.
[27] See GDPR, Article 4(1).
[28] See POPIA, section 1.

of the GDPR, to enumerate an open list of subsets of information which serve as examples of what definitively entails 'personal information'. Another example for a reference to 'personal information', which is defined as 'any information, including data, about an identified or identifiable natural person', can be found in Article 14.1 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Interestingly, in the California Consumer Privacy Act of 2018 (CCPA) 'personal information' is defined more specifically than in most instruments as 'information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household'.[29]

2.1.2.5.2 Non-personal data

The few times the term 'non-personal data' has been defined, it has been done for fairly specific purposes, usually by simply contrasting the term with 'personal data'. In other words, under these particular definitions at least, 'non-personal data' is all data that is not 'personal data'. For example, the European Union (EU) has adopted a regulation 'on a framework for the *free flow* of non-personal data in the European Union'[30] (EU NPDR) and clarified the term 'data' for purposes of this specific regulation, namely the free flow of 'non-personal data'.[31] It effectively defines 'non-personal data' as 'data other than personal data' with reference to the definition of 'personal data' in Article 4(1) of the GDPR.[32] Similarly, the Committee of Experts on a Non-Personal Data Governance Framework constituted by the Indian Ministry of Electronics and Information Technology (Indian NPD Committee) for purposes of making suggestions for consideration by the Indian government defines 'non-personal data' in two ways: first, as data that is not 'personal data' as defined in the Indian Personal Data Protection Bill and/or, second, as data 'without any personally identifiable information'.[33] Despite the fact that it is not always clear, as to whether particular data constitute 'personal data', we adopt a similar approach to 'non-personal data' from a legal standpoint, i.e. it

[29] See CCPA, § 1798.140(o)(1).
[30] Emphasis added.
[31] See EU NPDR, Article 3(1).
[32] See EU NPDR, Article 3(1).
[33] See Indian NPD Committee Report (2020) 13, paragraph 4.1(ii) <https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf> accessed 18 September 2022.

is data which does not constitute 'personal data'. This includes data which has been 'de-identified', 'anonymised' or 'pseudonymised'.[34]

2.1.2.5.3 Mixed data sets

'Mixed datasets' are sets of data which consist of both personal and non-personal data. The European Commission, for example, has stipulated as much in its 2019 guidance note on the EU NDPR and added that '[m]ixed datasets represent the majority of datasets used in the data economy and are common because of technological developments such as the Internet of Things (i.e. digitally connecting objects), artificial intelligence and technologies enabling big data analytics'.[35] To illustrate, the Commission provides a number of examples, including:

- → a company's tax record, mentioning the name and telephone number of the managing director of the company;
- → a research institution's anonymised statistical data and the raw data initially collected, such as the replies of individual respondents to statistical survey questions; and
- → analysis of operational log data of manufacturing equipment in the manufacturing industry.[36]

2.2 Data protection and data subjects

'Data protection' as used here is a term of art. The 'data' referred to are limited to *personal* data, with the word 'protection' alluding to the safeguarding of, or attempts to purportedly safeguard, personal data against its unauthorised use. In this context, we often refer to 'data subjects', by which we mean the persons to whom particular personal data pertain.

[34] In this regard, see for example the definition 'de-identify' in POPIA, section 1. See also KDPA, section 2, where 'anonymisation' is defined, and GDPR, Article 4(5), which defines 'pseudonymisation'.
[35] European Commission, Guidance on the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union (**European Commission Guidance Note**) <https://bit.ly/3qJOuf9> accessed 18 September 2022, section 2.2.
[36] European Commission Guidance Note, section 2.2.

2.3 Data localisation

As 'data localisation' is a more contested term, we opt for a broad descriptive definition in this report. It refers to measures that have the effect of limiting the flow of data to a certain locale, whether it be a country, set of countries, region, or even sub-national geographical units like states, provinces, or cities.

Data localisation measures come in various forms, each of which has its own set of consequences and peculiarities.[37] For example, some measures explicitly mandate localisation in one way or another. Some measures require that copies of specific types of data be stored on a server in a given geography, whereas others may ban the transfer of certain data types to other locales outright. The former category of measures results in a weaker form of localisation in the sense that the data in question may leave a particular jurisdiction, provided that a copy of that data remains in that jurisdiction. The latter category of measures is stronger because the data may not leave the jurisdiction at all. Measures that stipulate where data must be *stored* may go hand-in-hand with measures that speak to where certain types of data may be *processed*.

With other forms of data localisation, measures may simply unintentionally localise data as a by-product, with the predominant aim of the measure being something else entirely. For example, some countries require that other countries uphold certain minimum standards with respect to the privacy of individuals in relation to personal data that pertains to those individuals before that data will be permitted to be transferred across the border in question. The main aim of such measures is usually to ensure that when personal data travels across borders, the privacy of individuals is still protected in the jurisdiction to which it is transferred. That said, an unintended consequence of such measures can be some form of data localisation because of, for example, differences in the extent to which countries protect privacy, or the inability of one country to assure another that the privacy of the inhabitants of the latter will be adequately protected.

[37] For a good overview in this regard, see Dan Svantesson, 'Data Localisation Trends and Challenges: Considerations for the Review of the Privacy Guidelines', vol 301 (OECD Digital Economy Papers, No 301, OECD Publishing, Paris, 2020) <http://dx.doi.org/10.1787/7fbaed62-en> accessed 18 September 2022.

2.4 Cybersecurity

'Cybersecurity', also a significantly contested term,[38] relates to measures (purportedly) taken to safeguard data flows from unlawful access (often called 'cyber attacks'). This is not to be confused with who may (or may not), in a legal sense, use particular data. Rather, cybersecurity measures are generally aimed at ensuring that particular data is received by the intended recipient and are not intercepted or otherwise accessed by unintended persons such as hackers.

2.5 Digital trade

Digital trade encompasses the various subjects of trade (e.g., goods, services, or data) delivered via the internet and associated technologies (e.g., cloud computing services and voice-over-internet calls).[39] It is thus sometimes also called digitally enabled trade because it cannot occur in the absence of cross-border data flows.

2.6 Data protectionism, barriers to digital trade and restrictions to cross-border data flows which distort trade

While 'protectionism' has no official definition,[40] we broadly understand it as referring to measures that are intended to provide domestic economic actors with a competitive advantage vis-à-vis foreign economic actors with whom they are in a competitive relationship. The United States' (US) Office of the Special Trade Representative (now, the United States Trade Representative (USTR)) once clarified that this is sought to be achieved by adopting measures, which result in high barriers to trade when defining protectionism as 'the setting of trade barriers high enough to discourage imports or to raise their prices sufficiently to enable relatively inefficient domestic producers to

[38] See, for example, in this regard Ronald J Deibert, 'Toward a Human-Centric Approach to Cybersecurity' (2018) 32 Ethics & International Affairs 411, 411.

[39] For a similar definition, see Rachel F Fefer, Shayerah Ilias Akhtar and Wayne M Morrison, 'Digital Trade and U.S. Trade Policy' (Congressional Research Service, R44565, 2017) <https://bit.ly/3RUQxsx> accessed 18 September 2022.

[40] Swedish Board of Trade, 'Protectionism in the 21st Century' (Kommerskollegium 2016:2, 2016) <https://bit.ly/3dlJOsJ> accessed 18 September 2022; Robert W McGee, 'The Philosophy of Trade Protectionism, Its Costs and Its Implications' [1996] SSRN Electronic Journal <http://www.ssrn.com/abstract=91369> accessed 18 September 2022.

compete successfully with foreigners'.[41] Thus, protectionism in the international trade context is limited to cross-border exchanges.

Applied to the data economy, protectionism refers to measures (e.g., border measures or domestic policies) that aim at providing a competitive advantage to domestic economic actors vis-à-vis their foreign competitors when the former, depending on the type of data at issue, either trades in that data or uses data flows to transfer, transmit or deliver their product offerings. Therefore, data protectionism relates to digitally enabled trade. This might be the reason why data protectionism is occasionally also called digital protectionism.[42]

While data protectionism is sometimes conflated with the notion of trade barriers to cross-border data flows and deemed a new form of protectionism by a large number of authors,[43] the two ideas are conceptually distinct. To begin with, there is no such thing as *trade* barriers to cross-border data flows. In the data flow context, trade barriers are measures that distort the competitive conditions of the exchange of subjects of digital trade.[44] Since this sort of exchange requires cross-border data flows, these measures come in the form of trade distortive restrictions to data flows. Relevant trade distortive restrictions can be identified irrespective of a given government's intention to shield domestic economic participants from foreign competitors,[45] and irrespective of whether a given measure relates to imports or exports, has a protectionist effect or not, or is considered legitimate or illegitimate. Put differently, governments' intentions might be really hard

[41] United States Trade Representative, *A Preface to Trade* (US Government Publishing Office 1982) 149. But see Susan A Aaronson, *Taking Trade to the Streets: The Lost History of Public Efforts to Shape Globalization* (University of Michigan Press 2001) 9, where Aaronson contends that this definition is outdated without providing a suggestion for an updated one. The USTR's definition has evolved and does now equate protectionism with erection of trade barriers to digital trade, see below sections 3.1.1 and 3.2.1.

[42] Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (n 10) 543 refers in footnote 1 to a comparative google search in this regard.

[43] See, for example, Swedish Board of Trade (n 41); Henry S Gao, 'Google's China Problem: A Case Study on Trade, Technology and Human Rights under the GATS' (2011) 6 Asian Journal of WTO & International Health Law & Policy 347; and Fredrik Erixon and Hosuk Lee-Makiyama, 'Chinese Censorship Equals Protectionism' (6 January 2010) *The Wall Street Journal*.

[44] See in this regard Martina F Ferracane, 'The Costs of Data Protectionism' in Mira Burri (ed), *Big Data and Global Trade Law* (Cambridge University Press 2021).

[45] See Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (n 10) 546. We note, however, that it may be difficult to ascertain intent insofar as what governments want to protect is concerned.

to ascertain; as is whether certain measures relate to imports or exports, since data flows are fluid and frequent, and location is hard to determine on borderless networks.[46] Whether a distortion exists should thus hinge on whether a measure or set of measures provide a competitive advantage as a matter of fact as opposed to having to identify whether that measure or set of measures have, in a normative sense, been shielding domestic economic participants from foreign competitors or not.

An example of a measure providing a competitive advantage would be the idea of 'data protection'. The importing country may require foreign economic actors to show that they comply with a privacy standard that might provide domestic economic actors with a competitive advantage under certain circumstances. Further examples might be censorship measures since they reduce the platform's openness and impede universal access to information,[47] as well as the blocking and redirection of internet traffic,[48] and distributed denial-of-service (DDoS) attacks (that is bombarding a website with service requests) since it destabilises at least parts of the internet, disrupts communication, reduces data security, and increases costs.[49]

As for the perceived (il)legitimacy of a given distortive restriction, this is something which, in the absence of a clear shared understanding of what is and is not legitimate, will differ from jurisdiction to jurisdiction, and will usually be reflected in the public policy goals of individual jurisdictions as embodied in their rules and the exceptions to those rules.

---

[46] Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (n 10) 546.

[47] See Andrew McLaughlin, 'Censorship as Trade Barrier' <https://bit.ly/3Sbkq7Q> accessed 18 September 2022; Jonah Force Hill, 'The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders' (2014) 2 Lawfare Research Paper Series 1; Justin Clark and others, 'The Shifting Landscape of Global Internet Censorship' [2017] SSRN Electronic Journal <https://www.ssrn.com/abstract=2993485> accessed 18 September 2022.

[48] In 2007, Google asked the USTR to fight censorship as a trade barrier. See Christopher S Rugaber, 'Google Asks Gov't to Fight Censorship' <https://usatoday30.usatoday.com/tech/products/2007-06-22-2859711256_x.htm> accessed 16 September 2022.

[49] Carl Bildt, 'A Victory for the Internet' <https://www.nytimes.com/2012/07/06/opinion/carl-bildt-a-victory-for-the-internet.html> accessed 16 September 2022; Sarah Box, 'Internet Openness and Fragmentation: Toward Measuring the Economic Effects' <https://www.cigionline.org/sites/default/files/gcig_no.36_web.pdf> accessed 16 September 2022.

To draw lessons for regulating cross-border data flows in Africa, then, it is most useful for us to focus on specifically defined barriers to digital trade. In other words, it is best to examine identifiable types of restrictions to cross-border data flows that result in trade distortions, regardless of intention and regardless of whether they are deemed to be justifiable by one state (or set of actors within that state) and unjustifiable by others. This avoids having to rely on vague, disputed concepts such as 'data protectionism'.

3 Approaches towards restrictions and the free flow of data across borders

When regulating cross-border data flows, governments have taken different approaches towards trade distortive restrictions of cross-border data flows vis-à-vis its free flow at the national / supranational level (discussed in section 3.1), as opposed to at the international or regional level (discussed in section 3.2).

3.1 National / supranational level

Here, we start by looking at the way large, often dominant economies regulate cross-border data flows. Specifically, we examine the approaches of the US (in section 3.1.1), the EU (in section 3.1.2) and China (in section 3.1.3). We then turn to describe the regulation of cross-border data flows that exists in African jurisdictions (in section 3.1.4), with a particular focus on Kenya (in section 3.1.4.1), Nigeria (in section 3.1.4.2) and South Africa (in section 3.1.4.3).

3.1.1 United States

As Shaffer puts it, the US 'has trumpeted a world of free "data flows" that would benefit its companies'.[50] As such, while its views on what does and does not constitute a trade distortive restriction to cross-border data flows has constantly been evolving,[51] its general approach, at least

[50] Gregory Shaffer, 'Trade Law in a Data-Driven Economy: The Need for Modesty and Resilience' (2021) 20 World Trade Review 259, 269.

[51] For a good overview in this regard, see Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (n 10).

at the national level, has been to classify virtually all restrictions on cross-border data flows as being trade distortive and illegitimate[52] (i.e., being unjustifiable in terms of public policy goals). Restrictions of this kind include:

- → the imposition of tariffs on the subjects of digital trade;
- → all kinds of data localisation requirements;
- → the failure to protect intellectual property (IP) rights online;
- → 'burdensome' standards (for example standards which require firms to divulge source code);
- → internet filtering (including filtering used for the purposes of censorship);[53] and
- → cybersecurity rules.[54]

Consistent with its definitions and views, there are very little national-level regulations or policies in the US that can be viewed as constituting trade distortive restrictions to cross-border data flows.[55] The fact that today's largest economic players are mostly technology firms based in the US that are heavily reliant on cross-border data flows may explain why the US pushes for commitments ensuring that data flows as freely as possible across borders.

---

[52] On the US' perspective on what is legitimate regulation and what is trade distortive, see Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (n 10) 557 et seq.

[53] The US did explore challenging Chinese censorship policies, but without launching a trade dispute. See United States Trade Representative, 'United States Seeks Detailed Information on China's Internet Restrictions' (United States Trade Representative, 19 October 2011) <https://bit.ly/3BPjtN9> accessed 16 September 2022.

[54] See Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (n 10) 550; USITC 2013 (n 4) xxi.

[55] That said, individual states also have policy- and rule-making autonomy in relation to data. Such autonomy has been exercised in a number of states. The most prominent example in this regard is California, which passed the California Consumer Privacy Act (CCPA) in 2018. After being put to a ballot, the CCPA was subsequently amended with approval of voters by the California Privacy Rights Act (CPRA) in 2020. While the CCPA as amended contains a provision that impact the conditions under which data may flow across sub-national and national borders (see CPRA, section 1798.100(d)), we are not aware of any evidence to suggest that it was enacted with protectionist intent, nor that it results in any form of *de facto* protectionism because the provision in question imposes the same obligations in relation to data flows within California.

3.1.2 European Union

For the purposes of the regulation of cross-border data flows, acknowledging that the EU is a supranational organisation,[56] we regard the EU jurisdiction as a single market. The two main instruments in the EU which regulate cross-border data flows are the GDPR, which focuses on personal data flows, and the EU NPDR, which regulates non-personal data flows, i.e., it applies to all data flows to which the GDPR does not apply. Insofar as non-personal data is concerned, the EU NPDR promotes free cross-border data flows within the EU,[57] and considers only a small set of trade distorting restrictions as constituting legitimate restrictions to cross-border data flows (i.e., being justifiable in terms of public policy goals).[58]

The approach differs in relation to personal data. The primary purpose of the GDPR is to give effect to the fundamental right of privacy of persons living in the EU. Thus, it justifies the restriction of cross-border data flows when privacy protection is it at stake, even when such restrictions are trade distortive.[59] For example, the GDPR contains, amongst other things, seven articles in Chapter 5 that regulate transfers of personal data to third countries or international organisations.[60] Article 44 makes '[a]ny transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation', inter alia, subject to the fact that the conditions laid down in the following provisions of

Chapter 5 are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third

[56] A supranational organisation is an international organisation, or union, whereby a set of individual countries agree to make rules which transcend national boundaries and which to varying degrees binds the entire group of countries.
[57] See EU NPDR, Article 1, which provides that its aim is 'to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localisation requirements, the availability of data to competent authorities and the porting of data for professional users'.
[58] EU NPDR, Article 4(1), for example, provides that '[d]ata localisation requirements shall be prohibited, unless they are justified on grounds of public security in compliance with the principle of proportionality', thus significantly curtailing the ability of EU member states to distort intra-EU trade via imposing restrictions on cross-border data flows.
[59] See, for example, Christian Peukert and others, 'Regulatory Export and Spillovers: How GDPR Affects Global Markets for Data' <https://voxeu.org/article/how-gdpr-affects-global-markets-data> accessed 18 September 2022; Daniel Lyons, 'GDPR: Privacy as Europe's Tariff by Other Means?' <https://www.aei.org/technology-and-innovation/gdpr-privacy-as-europes-tariff-by-other-means/> accessed 18 September 2022.
[60] See GDPR, Articles 44 to 50.

country or to another international organisation … to ensure that the level of protection of natural persons guaranteed by [the GDPR] is not undermined.

Therefore, the provisions in Articles 45 to 50 include what the EU views as legitimate reasons to restrict cross-border data flows, including when they are trade distortive. According to Article 45, the European Commission may only authorise cross-border data transfer to third countries if a given third country provides an 'adequate level of protection' (through so-called adequacy decisions).[61] Thereafter, such transfers may take place without any prior authorisation from a supervisory authority,[62] but must be periodically reviewed.[63] A comprehensive list in paragraph 2 stipulates what the European Commission 'shall … take account of' when assessing the adequacy of the level of protection, including

> the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation …, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.[64]

The list also includes the existence and effective functioning of an independent supervisory authority responsible 'for ensuring and enforcing compliance' with data protection rules as well as international commitments of the third country in this regard.[65] This provides the European Commission with extensive discretion to determine whether to authorise the transfer of data to third countries, which may translate into restrictions on the flow of data across borders, which are trade distortive.

[61] See GDPR, Article 45(1), sentence 1.
[62] See GDPR, Article 45(1), sentence 2.
[63] See GDPR, Article 45(4).
[64] Article 45(2), bullet 1.
[65] Article 45(2), bullets 2 and 3.

In the absence of authorisation by the European Commission, based on an 'adequate level of protection', cross-border data flows may still take place if the controller or processor of the data provides for 'appropriate safeguards' and 'on condition that enforceable data subject rights and effective legal remedies for data subjects are available'.[66] These requirements may in some instances constitute a restriction to cross-border data flows, which are trade distortive, and the EU seems to view such restrictions as legitimate. Paragraph 2 of Article 46 stipulates instances in which 'appropriate safeguards' are sufficient to enable transfers without the need for prior authorisation by the Commission, while paragraph 3 provides instances in which prior authorisation is necessary.

Article 49 of the GDPR indicates when one may derogate from Articles 45 and 46, i.e. it provides for instances in which neither an adequate level of protection nor appropriate safeguards are necessary to transfer data to third countries. These instances include situations where:

- → the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;[67]
- → the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;[68]
- → the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;[69]
- → the transfer is necessary for important reasons of public interest;[70] and
- → the transfer is necessary for the establishment, exercise or defence of legal claims.[71]

[66] Article 46(1).
[67] Article 49(1)(a).
[68] Article 49(1)(b).
[69] Article 49(1)(c).
[70] Article 49(1)(d).
[71] See GDRP, Article 49(1)(e).

While the GDPR has the stated aim of protecting the fundamental right to privacy, it can also result in trade distortive restrictions to cross-border data flows, whether intended or not, and whether considered appropriate in the context of the GDPR or not. As such, the GDPR has the propensity to impose additional costs on firms that rely on extra-EU data flows. This provides competitive advantages to firms that merely rely on intra-EU data flows, and thus alters the conditions of competition between the former set of firms and the latter.

3.1.3 China

China's regulation of cross-border data flows is protectionist in nature and intent, and consists of measures, which clearly constitute trade distortive restrictions to cross-border data flows. It provides clear and significant competitive advantages to Chinese firms vis-à-vis non-Chinese firms. To achieve this, it imposes various '"data localization" requirements on sovereignty grounds, rather than the protection of citizen rights'.[72] Such requirements limit access to Chinese nationals' data to Chinese firms. This results in the Chinese government and Chinese firms controlling the data of China's citizens (which is over 1.4 billion people), facilitating social control on the government's side and, simultaneously, creating a significant competitive advantage for Chinese firms, in large part because of the sheer size of China's population.[73] Undoubtedly, this advantage has contributed to the development of large, internationally competitive digital multinational enterprises (MNEs), some of which are now as valuable as some of their US counterparts. Examples are the Chinese information technology titans Alibaba and Tencent.

Chinese data flow policy is regulated by a wide array of legal instruments. The Chinese Cybersecurity Law of 2017 (CCL) states that '[c]ritical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, *shall* store it within mainland China'.[74] The term 'important data' is not defined in the CCL, but clarified in the draft Implementing Measures on Data

[72] Shaffer (n 51) 269.
[73] Shaffer (n 51) 269.
[74] CCL, Article 37. Emphasis added.

Security Management (**CCL DSM Draft Measures**). Accordingly, 'important data' refers to 'data that, if divulged, may directly affect national security, economic security, social stability, or public health and safety, such as undisclosed government information or large-scale data on the population, genetic health, geography, mineral resources', but 'does not include enterprises' production, operations, and internal management information, personal information'.[75] Moreover, the term 'critical information infrastructure operators' is defined in the Implementing Cybersecurity Review Measures (**CCL CR Measures**) as 'operators designated by CII protection work departments'.[76] While 'CII' refers to 'critical information infrastructure',[77] there is no further information regarding the 'CII protection work departments'. Notably, given that 'network operators' are defined in the CCL as 'network owners, managers, and network service providers',[78] they cannot be equated with 'critical information infrastructure operators'. All in all, the Chinese approach to data localisation requirements extends well beyond the protection of personal data,[79] as it also goes to 'important data' and leaves the government with very broad discretion when it comes to implementing the law.

More recently, and in addition to the CCL, the Chinese government has passed the Data Security Law (**DSL**) and the Personal Information Protection Law (**PIPL**), which came into effect on 1 September 2021 and 1 November 2021 respectively. Both provide clarity in respect of various regulatory issues. For example, and interestingly, according to Article 11 of the DSL '[t]he State is to actively engage in international exchanges and cooperation in fields such as data security governance and data development and use'. This includes 'participating in the formulation of international rules and standards related to data security, and promoting the secure and free flow of data across borders'.[80] Moreover, Article 31 of the DSL reaffirms that '[t]he provisions of the

[75] CCL DSM Draft Measures, Article 38(5).
[76] See CCL CR Measures, Article 20.
[77] See CCL CR Measures, Article 1.
[78] See CCL, Article 76(3).
[79] It should, however, be added that China has recently passed the Personal Information Protection Law of 2021, which may itself be applied in ways which amount to further *de facto* data localisation measures being imposed in relation to personal data.
[80] DSL, Article 11.

[CCL] apply to the outbound security management … of important data collected or produced by critical information infrastructure operators operating within the mainland territory of [China]'. 'Outbound security management' refers to 'the security procedures and rules involved in transfer of data out of the mainland territory of [China]'.[81]

Furthermore, Chapter III of the PIPL includes a variety of rules on the cross-border transfer of personal data, including providing a high level of personal data protection.[82] While modelled after the GDPR,[83] there are distinct differences between the PIPL and the GDPR. For example, Article 38 of the PIPL indicates a clear preference for personal data not leaving China when it indicates that one of a number of conditions must be met '[w]here personal information handlers *truly need to provide personal information outside the borders of the People's Republic of China for business or other such requirements*'.[84] All of these conditions also illustrate a clear difference between the approaches taken in the GDPR and the PIPL. The PIPL, for example, requires (i) '[p]assing a security assessment organised by the State cybersecurity and informatization department';[85] (ii) '[u]ndergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department';[86] or (iii) '[c]oncluding a contract with the foreign receiving side in accordance with a standard contract formulated by the State cyberspace and informatization department'.[87] Article 43 additionally allows China to adopt reciprocal measures against a country or region that adopts discriminatory measures vis-a-vis China when the discrimination relates to personal information protection. None of the above legal provisions have analogues in the GDPR.

[81] DSL, Article 31.
[82] See PIPL, Articles 38 through 43.
[83] See, for example, Skadden, Arps, Slate, Meagher & Flom LLP, 'China's New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies' (Skadden Insights) <https://bit.ly/3xy8Pb0> accessed 18 September 2022.
[84] Emphasis added.
[85] PIPL, Article 38(1).
[86] PIPL, Article 38(2).
[87] PIPL, Article 38(3).

The way China has governed cross-border data flows has formed a strong part of its digital industrial policy strategy, and the above laws and measures, which are but a subset of all the tools at the government's disposal, begin to illustrate how, particularly in contrast to the US approach, the Chinese government enjoys far reaching discretion to continue protecting its domestic industries that rely on cross-border data flows. The government has used this discretion in a protectionist manner and has, to a large extent, achieved its digital industrial policy and developmental goals.

3.1.4 African jurisdictions

Not many African countries have legislation that directly regulate cross-border data flows. Sixty-one percent of African countries have legislation regulating electronic transactions, 52 percent have legislation on digital consumer protection, 61 percent have legislation relating to privacy and data protection and 72 percent have cybercrime legislation.[88] Moreover, the design and implementation of existing legislation, quite often, differs rather significantly from country to country. For example, in relation to enforcing data protection rules, Ghana and Mauritius issue fines for non-compliance,[89] whereas legislation in Morocco, Nigeria, Senegal and Tunisia do not require notification of breaches.[90] What this begins to illustrate is that, though some countries on the continent have taken similar approaches to data governance in certain respects, overall, there are significant differences in approaches between African countries. In this section, then, we speak only to the approaches that have been adopted in Kenya (section 3.1.4.1), Nigeria (section 3.1.4.2) and South Africa (section 3.1.4.3). We have selected these jurisdictions because these countries are three of Africa's largest economies, with each hailing from a different region on the continent and each having taken its own path. While we do not discuss the approaches of other countries,

[88] Data sourced from United Nations Conference on Trade and Development, 'UNCTAD Global Cyberlaw Tracker: Summary of Adoption of E-Commerce Legislation Worldwide' (2021) <https://bit.ly/3qO3BnO> accessed 18 September 2022.

[89] Deloitte, 'Privacy Is Paramount: Personal Data Protection in Africa' <https://bit.ly/2IdfBrI> accessed 17 September 2022.

[90] Tomiwa Ilori, 'Data Protection in Africa and the COVID-19 Pandemic: Old Problems, New Challenges and Multistakeholder Solutions' (Association for Progressive Communications) <https://bit.ly/3UuDmQW> accessed 18 September 2022.

the same applies to them as well, which ultimately means that one cannot currently speak of a unified African approach to the regulation of cross-border data flows.

3.1.4.1 Kenya

The Kenya Data Protection Act (KDPA) of 2019 is the central instrument of the Kenyan data regulatory framework. Its objects and purposes are to regulate the processing of *personal* data (i.e., 'any information relating to an identified or identifiable natural person'),[91] with a view to protecting the privacy of individuals.[92] Notably, section 2 of the KDPA includes the idea of 'health data' as a subset of personal data, which relates to

> the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.

Moreover, section 2 seems to distinguish between sensitive and non-sensitive personal data by stipulating that 'sensitive personal data' refers to data revealing '[a] natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject'[93] without defining non-sensitive data. By implication, all data that is not sensitive personal data constitutes non-sensitive personal data.

Against this backdrop, then, 'data' for purposes of the KPDA is information which:

- → is processed by means of equipment operating automatically in response to instructions given for that purpose;
- → is recorded with intention that it should be processed by means of such equipment; and
- → is recorded as part of a relevant filing system.[94]

[91] See KDPA, section 2.
[92] See KDPA, preamble. On the full 'object and purpose' of the KDPA, see further KDPA, section 3.
[93] See KPDA, section 2.
[94] See KPDA, section 2.

Where information does not fall under any of these categories, it is considered data when it:

→ forms part of an accessible record; or

→ is recorded information which is held by a public entity.[95]

Accordingly, if a school records a list of its students' names, identity numbers, sex and other information, the recording of the information would constitute 'data' in a countable sense. However, amounts of information fed through a machine learning system for analytic purposes would, for example, equally be viewed as data, i.e., 'data' in the mass noun sense as virtually uncountable. Therefore, the KPDA regulates personal data in both the countable and mass noun forms of the term.

There is no legislation in Kenya governing cross-border transfers of non-personal data. This means that, as a general proposition, there is currently no explicit legislative basis for Kenya to engage in data protectionism insofar as non-personal data is concerned.

As for personal data, the KDPA explicitly includes applicable provisions on cross-border transfers of data and *de jure* data localisation. Section 48 of the KPDA makes the transfer of personal data to other countries conditional on appropriate safeguards with respect to the security and protection of personal data being in place in the foreign country in question unless the transfer is 'necessary' for several enumerated reasons, including:

→ the performance of contracts, for matters of public interest;

→ for the establishment, exercise, or defence of a legal claim; and

→ for the 'purpose of compelling legitimate interests pursued by the data controller or data processor which are not overridden by the interests, rights and freedoms of the data subjects'.96

Section 49 does not only require additional safeguards in the context of 'sensitive' personal data, but empowers the Data Commissioner to:

[95] See KPDA, section 2.
[96] See further KDPA, section 48(c).

→ request persons transferring data out of Kenya to demonstrate that it has complied with certain elements of section 48; and

→ prohibit, suspend, or subject a transfer to such conditions as may be determined to protect the rights and fundamental freedoms of data subjects.

Sections 48 and 49 read together makes it clear that the Data Commissioner has the discretion to determine what constitutes appropriate safeguards with respect to the security and protection of personal data. The way the Data Commissioner exercises this discretion could lead to *de facto* localisation of personal data and, thus, restrict cross-border data flows. This might, in turn, intentionally or unintentionally, provide advantages to data processors that rely on data transfers within Kenya vis-à-vis their competitors that rely on cross-border transfers out of Kenya. This could *de facto* amount to discrimination between domestic and foreign data processors and, therefore, restrict cross-border data flows in a trade distorting way, especially if the Data Commissioner sets a high standard in relation to what constitutes appropriate safeguards.

Additionally, section 50 of the KDPA explicitly enables the relevant Cabinet Secretary to 'prescribe, based on grounds of strategic interests of the state or protection of revenue, certain nature of processing that shall only be effected through a server or a data centre located in Kenya'. This empowers the Cabinet Secretary to impose explicit storage and processing localisation requirements through enacting regulations, especially since 'processing' is defined in the KPDA broadly.[97] To this end, the Cabinet Secretary has recently finalised the Data Protection (General) Regulations (KDPA Regulations), which includes provisions that affect the implementation of sections 48, 49 and 50 of the KDPA.

Regulations 39 to 48 of the KDPA Regulations provide more specific conditions for when personal data may be transferred out of Kenya. Whether too onerous or not for achieving the aims of the Act, these additional conditions could have an impact on the competitive relationship between personal data processors relying merely on data transfers within Kenya vis-à-vis their

[97] See KDPA, section 2.

competitors that rely on cross-border transfers out of Kenya and, thus, possibly *de facto* between those based in Kenya and those based elsewhere.

Regulation 40, for example, requires that a data controller or data processor, before transferring personal data out of Kenya, ascertains that the transfer is based on one of the following grounds:

> (a) appropriate data protection safeguards;
>
> (b) an adequacy decision made by the Data Commissioner;
>
> (c) transfer as a necessity; or
>
> (d) consent of the data subject.

In practice, this can play out in many ways, and might, in a variety of circumstances, result in intended or unintended restrictions of cross-border data flows that are trade distortive. For example, it may be that obtaining 'consent' from data subjects is so easy that there are no associated costs resulting in a competitive advantage for firms relying purely on intra-Kenya data flows. It is also possible, however, that data subjects do not consent. This would mean that the data would effectively be localised or, at the very least, prohibited from flowing out of Kenya to foreign countries. Since section 2 of the KDPA defines consent in a fairly robust way, i.e., as 'any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject'. Arguably, many firms will fail to obtain the necessary consent in a legal sense.

Another example is ensuring that 'appropriate data protection safeguards' are in place prior to a cross-border personal data transfer. Regulation 41(1) of the KDPA Regulations indicates that such safeguards are appropriate where:

> (a) the intended recipient is subject to a legal binding instrument that contains equivalent safeguards of the KPDA and its Regulations; or

> (b) the data controller has 'assessed all the circumstances surrounding transfers of that type of personal data to another country' and concludes that appropriate safeguards exist.

Such vague stipulations invite a broad set of possible interpretations. Legal advice on whether a company is compliant with section 41(1) or not might not only be a costly exercise but entails a certain amount of risk. The advice may turn out to be incorrect before a relevant court, in which case the company may be held liable and may, in turn, incur additional costs.

The administrative burden, which might turn out to be incredibly costly, increases even more if the cross-border data transfer takes place in reliance on a sub-regulation. Regulation 41(2) of the KDPA Regulations additionally requires that:

> (a) the transfer shall be documented;
>
> (b) the documentation shall be provided to the Commissioner on request; and
>
> (c) the documentation shall include
>
> (i) the date and time of the transfer;
>
> (ii) the name of the recipient;
>
> (iii) the justification for the transfer; and
>
> (iv) a description of the personal data transferred.

Finally, it is worth mentioning that section 50 of the KPDA must be read together with regulation 26 of the KDPA Regulations. Section 50 of the KPDA, as mentioned above, contains a general provision that empowers the Cabinet Secretary to impose localisation requirements through legislation, with regulation 26(1) explicitly imposing storage and processing localisation requirements in relation to scenarios of 'strategic interest of the state'. These include matters relating to legal identity management, elections, the administration of public finances, early childhood education and the provision of primary or secondary healthcare.[98] Importantly, it also

[98] See KDPA Regulations, where regulation 26(2) provides an open-ended list.

includes 'running any system designated as a protected computer system in terms of section 20 of the Computer Misuse and Cybercrime Act, 2018 [the CMCA]'.[99] Section 20 of the CMCA, in turn, defines 'protected computer system' as a 'computer used directly in connection with, or necessary for':

(a) the security, defence or international relations of Kenya;

(b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law;

(c) the provision of services directly related to communications infrastructure, banking and financial services, payment and settlement systems and instruments, public utilities or public transportation, including government services delivered electronically;

(d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services;

(e) the provision of national registration systems; or

(f) such other systems as may be designated relating to the security, defence or international relations of Kenya, critical information, communications, business or transport infrastructure and protection of public safety and public services as may be designated by the Cabinet Secretary responsible for matters relating to information, communication and technology.

The final sub-section listed above, i.e., section 20(f), provides the relevant Cabinet Secretary significant latitude in defining what constitutes a 'protected computer system' such that storage and processing localisation could result in restrictions to cross-border data transfers that are trade distortive. Notably, the same Cabinet Secretary responsible for and overseeing the KDPA and KDPA Regulations is also responsible for overseeing the CMCA. This is a similar approach to the one that has been adopted in China, central to which is the notion of 'critical information infrastructure', which, as indicated above, has been implemented in ways which protect firms that rely on intra-

[99] See KDPA Regulations, regulation 26(2).

Chinese data transfers as opposed to data transfers to territories outside of China. That said, while the regulatory framework does make this a distinct possibility, there is no indication thus far that the Cabinet Secretary will use the discretion afforded by the KDPA, KDPA Regulations and CMCA to protect Kenyan firms.

We are not suggesting that any provisions of the KDPA are unnecessary or unwarranted to protect privacy as a constitutional right. On the extent to which it might be an effective way to approach the protection of personal data, there is insufficient empirical data to even begin to undertake a proper assessment. However, the KDPA does at the very least seem, with some exceptions,[100] to have the propensity to privilege data flows within Kenya over data flowing elsewhere. This might result in *de facto* protection being accorded to Kenyan firms.

3.1.4.2 Nigeria

Nigeria has had certain specific data localisation regulations in place for some time. For example, the Central Bank of Nigeria imposed mandatory Guidelines on Point of Sale (POS) Card Acceptance Services in 2011. One provision, guideline 4.4.8, stipulates that '[a]ll domestic transactions including but not limited to POS and ATM transactions in Nigeria must be switched using the services of a local switch and shall not under any circumstance be routed outside Nigeria for switching between Nigerian Issuers and Acquirers'.

Another example is the mandatory Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) in 2013 (2013 NITDA Guidelines) imposed by the National Information Technology Development Agency (NITDA). The guidelines aim, among other things, at '[stimulating] and [increasing] the production, sales and consumption of high quality information technology products and services developed by indigenous companies that serve the unique needs of the local and global market'.[101] The 2013 NITDA Guidelines contain a

[100] It is, for example, possible for the Data Commissioner to make an adequacy decision, or for countries to enter into reciprocal data protection agreements with Kenya, or for countries to ratify the Malabo Convention. In these instances, data flows to other countries may be on an equal footing. The extent to which these scenarios will come into play remain to be seen.

[101] 2013 NITDA Guidelines, guideline 5.2.

number of localisation provisions, including guideline 12.1(4), which requires ICT companies to host all subscriber and consumer data in Nigeria. Guideline 14.2(3), moreover, requires all ministries, departments, and agencies of Nigeria's federal government to '[e]nsure that all government data is hosted locally inside the country'. Such localisation requirements are clear restrictions of cross-border data flows, which might turn out to be *de facto* disadvantageous for foreign IT firms, thus rendering the restrictions trade distortive.

The NITDA also issued the Nigeria Data Protection Regulation in 2019 (**NDPR**), which purportedly 'applies to natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria'.[102] It contains provisions on the transfer of data from Nigeria to other jurisdictions. Specifically, regulation 2.11 of the NDPR stipulates that personal data transferred to foreign countries are subject to the NDPR and that such transfers fall under the supervision of the NITDA and the Honourable Attorney General of the Federation (**HAGF**). It further requires the NITDA and the HAGF to undertake adequate level of protection assessments, in which listed factors have been considered.[103]

Regulation 2.12 provides for exceptions in situations where no determination of an adequate level of protection must be made.[104] Specifically, in the absence of an adequacy determination, 'a transfer or a set of transfers of Personal Data to a foreign country or an international organisation shall take place only on one [of the conditions stipulated in a sub-regulation]'. These conditions are as follows:

- → the data subject has 'explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers';[105]
- → the transfer is 'necessary' for the performance of certain contracts;[106]

[102] NDPR, regulation 1.2(b).
[103] NDPR, regulation 2.11(b).
[104] For a lengthier description of the NDPR, see Olumide Babalola, 'Nigeria's Data Protection Legal and Institutional Model: An Overview' (2022) 12 International Data Privacy Law 44.
[105] NDPR, regulation 2.12(a).
[106] NDPR, regulations 2.12(b) and (c).

→ the transfer 'is necessary for important reasons of public interest';[107]

→ the transfer is 'necessary for the establishment, exercise or defence of legal claims';[108] and/or

→ the transfer is necessary to protect the 'vital interests' of the data subject or of 'other persons' in situations where the data subject is 'physically or legally incapable of giving consent'.[109]

In 2020, a comprehensive Nigerian Data Protection Bill (**NDPB**) was published for comment. The NDPB contemplated the creation of a Data Protection Commission (**DPC**), which would have rendered the NDPR nugatory and transferred the function of personal data protection from the NITDA to the DPC. However, in late 2021, the Nigerian government abandoned the NDPB, indicating that it would seek to engage consultants to draft a new bill.[110] Therefore, the NDPR remains the primary regulatory instrument in Nigeria in relation to personal data, which might be used to *de facto* privilege local firms that rely on data flows within Nigeria much in the way the KDPA allows. Attention must be paid to the NDPB's successor bill, which might give further insights into how the Nigerian government currently thinks about data protection, and, potentially, trade distortive restrictions to cross-border data flows more generally.

As in the case of the KDPA, we are not suggesting that any provisions of the NDPR are unnecessary or unwarranted to give effect to the constitutional right to data protection. On the extent to which it might be an effective way to approach the protection of personal data, there is insufficient empirical data to begin to undertake a proper assessment. However, as in the case of the KDPA, the NDPR does at the very least seem to have the propensity to privilege data flows within Nigeria over data flowing elsewhere. This might result in *de facto* protection being accorded to Nigerian firms.

[107] NDPR, regulation 2.12(d).
[108] NDPR, regulation 2.12(e).
[109] NDPR, regulation 2.12(f).
[110] See Tosin Omoniyi, 'Data Protection: Indignation as FG Abandons Draft Bill, Seeks "Consultants" for Fresh Process' *Premium Times* <https://bit.ly/3RU6Iq8> accessed 18 September 2022.

3.1.4.3 South Africa

The current South African data regulatory regime is far simpler than its Kenyan and Nigerian counterparts. As in the case of Kenya, South Africa currently only regulates cross-border transfers of *personal* data, which means that the government does not have an explicit legislative mandate to regulate cross-border flows of non-personal data in ways that distort trade. Insofar as personal data is concerned, the central regulatory instrument in South Africa is the Protection of Personal Information Act of 2013 (POPIA), which came into effect in 2020. POPIA only applies to 'personal information', which is defined as 'information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person'.[111] It subsequently lists examples of personal information, including information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.[112] Notably, POPIA does not apply to personal information 'that has been de-identified to the extent that it cannot be re-identified again'.[113]

Section 72 of POPIA, which is the only section in Chapter 9 of the Act that is headed 'Transborder Information Flows', generally prohibits the transfer of personal data out of South Africa, unless one of the following circumstances is applicable:

- → a foreign recipient of personal information is subject to a law, binding corporate rules or binding agreement which provide an 'adequate level of protection';[114]
- → the data subject consents to the transfer;[115]
- → the transfer is necessary for the performance of certain types of contracts;[116]
- → the transfer is for the 'benefit of the data subject', it is not 'reasonably practicable to obtain the consent of the data subject to that transfer', and if it were

[111] POPIA, section 1.
[112] See further POPIA, section 1.
[113] POPIA, section 6(1)(b).
[114] See further POPIA, section 72(1)(a) where additional details are provided on what suffices as an 'adequate level of protection'.
[115] POPIA, section 72(1)(b).
[116] POPIA, sections 72(1)(c) and (d).

> reasonably practicable to obtain such consent, the data subject 'would be likely to give it'.[117]

As in the case of the KDPA and NDPR, we are not suggesting that any provisions of the POPIA are unnecessary or unwarranted to, as in the case of the KDPA and NDPR, protect privacy or related constitutional rights. On the extent to which POPIA might be an effective way to approach the protection of personal data, there is insufficient empirical data to begin to undertake a proper assessment. However, as in the case of the KDPA and NDPR, POPIA does, at the very least, seem to have the propensity to privilege data flows within South Africa over data flowing out of the country. This might result in *de facto* protection being accorded to South African firms.

Moreover, in April 2021, the South African Department of Communications and Digital Technologies published the Draft National Data and Cloud Policy (Draft NDCP). Thus, there might be a few policy interventions implemented soon, including that:

- → all data that form part of South Africa's 'critical information infrastructure' shall be processed and stored within the borders of South Africa;
- → a copy of all personal data transferred out of South Africa must be stored in the country for the purposes of law enforcement; and
- → '[t]o ensure ownership and control':
  - 〉 data generated in South Africa shall be the property of South Africa, regardless of where the technology company is domiciled.
  - 〉 government shall act as a trustee for all government data generated within the borders of South Africa.
  - 〉 all research data shall be governed by the Research Big Data Strategy of the Department of Science and Innovation (DSI).

[117] POPIA, section 72(1)(e).

- all data generated from South African natural resources shall be [co-owned] by government and the private sector participant/s whose private funds were used to generate such, and a copy of such data shall be stored in the [High-Performance Computing and Data Processing Centre].
- ownership and control of personal information and data shall be in line with the POPIA.
- the Department of Trade, Industry and Competition through the Companies and Intellectual Property Commission (CIPC) and the National Intellectual Property Management Office (NIPMO) shall develop a policy framework on data generated from intellectual activities including sharing and use of such data.[118]

While it remains to be seen whether and to what extent the Draft NDCP will be converted into a final set of policies and/or laws, there might soon be changes to the South African regulatory regime. This may provide a grounding for greater levels of restrictions to cross-border data flows that are trade distortive.

3.2 International / regional level

We turn next to examine the approaches of the same jurisdictions discussed above at the international and, where applicable, regional levels when regulating cross-border data flows. Again, we start by looking at the approaches of the US (in section 3.2.1), the EU (in section 3.2.2) and China (in section 3.2.3) before turning to look at African jurisdictions (in section 3.2.4).

3.2.1 United States

US practice at the international level reflects its regulatory preference for free cross-border data flows. This is evident from its approach in several FTAs, including the CPTPP, United States-Mexico-

[118] Draft NDCP, paragraph 10.4.

Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement. All these agreements include an obligation not to restrict cross-border data flows (including personal data flows) as a general rule, exceptions from this obligation in exceptional circumstances – including fairly detailed guidance in relation to what constitutes 'exceptional circumstances' – and an article on the protection of 'personal information'. Let's take the USMCA as an example.[119]

Article 19.11(1) prohibits countries from 'restrict[ing] the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person'. In paragraph 2, a general exception has been inserted for cases where restrictions are 'necessary to achieve a legitimate public policy objective'. Since the parties have not agreed on specific legitimate objectives, it seems that each government is permitted to determine what they consider a legitimate public policy objective, including their own level of protection, as long as the 'restrictions on transfers of information [are not] greater than are necessary to achieve the objective'.[120] This is subject to the measure not being 'applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade', terminology that is borrowed from introductory clause of Article XX of the General Agreement on Trade and Tariffs 1994 (GATT).

In Article 19.8(1), the Parties then recognise 'the economic and social benefits of protecting the personal information of users of digital trade and the contribution that this makes to enhancing consumer confidence in digital trade' and undertake to adopt or maintain a legal framework that provides such protection.[121] When doing so,

> each Party should take into account principles and guidelines of relevant international bodies … such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).[122]

[119] But see CPTPP, Articles 14.8 and 14.11; US-Japan Digital Trade Agreement, Articles 11 and 15.
[120] USMCA, Article 19.11(2).
[121] USMCA, Article 19.8(2).
[122] USMCA, Article 19.8(2).

According to Article 19.8(3), such 'principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability'. Moreover, the Parties recognise 'the importance of ensuring compliance with measures to protect personal information', while 'ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented'. However, Article 19.8(4) requires the Parties merely to 'endeavour to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction'.

3.2.2 European Union

Due to the GDPR being a general data protection law grounded in fundamental rights, the EU approach in negotiating its FTAs is more restrictive than the US's approach of prohibiting restrictions on cross-border data flows, including personal data flows, as a default. Instead, the EU proposes, as a starting point, a closed list of instances when data flows shall not be restricted between the parties to the agreement, implying that all other restrictions are generally acceptable (with some leeway provided for adding additional items to what will remain a closed list). Let's take the FTA negotiations between the EU and Indonesia as an example. It appears to instructively reflect the EU position.

The EU wishes to start with the protection of personal data and privacy. It does so by stating that '[e]ach Party recognises that the protection of personal data and privacy is a fundamental right and that high standards in this regard contribute to trust in the digital economy and to the development of trade'.[123] The proposed article continues in its second paragraph by explicitly permitting each Party to 'adopt and maintain the safeguards it deems appropriate to ensure the protection of personal data and privacy, including through the adoption and application of rules for the cross-border transfer of personal data'. It adds that '[n]othing in this agreement shall affect the protection

[123] See 'EU proposal for provisions on Cross-border data flows and protection of personal data and privacy' in relation to its ongoing FTA negotiations with Indonesia (**EU-Indonesia FTA Data Chapter Proposal**), Article 2(1) <https://bit.ly/3BOnD7Q> accessed 17 September 2022.

of personal data and privacy afforded by the Parties' respective safeguards'.[124] In addition, the EU proposes that such safeguards should not be subject to regulatory cooperation.[125]

Still, in general, the EU seems to regard the unrestricted flow of data across borders to be important by suggesting that the Parties commit 'to ensuring cross-border data flows to facilitate trade in the digital economy'.[126] To that end, the EU proposes to prohibit restrictions to cross-border data flows that require:

- → the use of computing facilities or network elements in the Party's territory for processing, including by imposing the use of computing facilities or network elements that are certified or approved in the territory of the Party;[127]
- → the localisation of data in the Party's territory for storage or processing;[128]
- → prohibiting storage or processing in the territory of the other Party;[129] and
- → making the cross-border transfer of data contingent upon use of computing facilities or network elements in the Party's territory or upon localisation requirements in the Party's territory.[130]

3.2.3 China

China continues, at least for the time being, to opt for using its domestic laws to regulate both the protection of personal data and data flows generally. Apart from some soft law provisions regarding the protection of personal information that are included in FTAs in which it is participating,[131] China

[124] EU-Indonesia FTA Data Chapter Proposal, Article 2(2).
[125] EU-Indonesia FTA Data Chapter Proposal, Article X(3).
[126] EU-Indonesia FTA Data Chapter Proposal, Article 1(1).
[127] EU-Indonesia FTA Data Chapter Proposal, Article 1(1)(a).
[128] EU-Indonesia FTA Data Chapter Proposal, Article 1(1)(b).
[129] EU-Indonesia FTA Data Chapter Proposal, Article 1(1)(c).
[130] EU-Indonesia FTA Data Chapter Proposal, Article 1(1)(d).
[131] For example, Article 12.8(1) of the China-Australia FTA indicate that '[n]otwithstanding the differences in existing systems for personal information protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal information of users of electronic commerce'. Paragraph 2 of the same Article provides that '[i]n the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organisations'. Accordingly, each part retains significant discretion in relation to the way it approaches the protection of personal information, as well as flexibility in the sense that each party need only take international standards and criteria into account, and only 'to the extent possible'.

has, thus far, not made any commitments in its FTAs in relation to cross-border data flows that truly constrain the highly trade distortive way it approaches restrictions to cross-border data flows. The closest China has come to submitting to rules in this regard is in the Regional Comprehensive Economic Partnership Agreement (RCEP Agreement), which came into effect in January 2022. Its Article 12.15(2), for example, provides that '[a] Party shall not prevent cross-border transfer of information by electronic means where such activity is for the conduct of the business of a covered person'.

Article 12.15(1), however, indicates that '[t]he Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means', with Article 12.15(3)(a) further indicating that '[n]othing in this Article shall prevent a Party from adopting or maintaining: any measure inconsistent with paragraph 2 that it considers necessary to achieve a legitimate public policy objective,[14] provided that the measure is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade'. Footnote 14 further clarifies that '[f]or the purposes of this subparagraph, the Parties affirm that *the necessity behind the implementation of such legitimate public policy shall be decided by the implementing Party*'.[132] Article 12.15(3)(b) adds that nothing shall prevent a party from taking 'any measure that it considers necessary for the protection of its essential security interests', importantly stipulating that '[s]uch measures shall not be disputed by other Parties'. In other words, in many instances China's approach to cross-border data flow restrictions would likely violate paragraph 2 of Article 12.15, though this would not matter very much. It may justify its approach on the basis of the self-judging public policy clause (in paragraph 3(a)) or on the basis of the essential security interests clause (in paragraph 3(b)).

[132] Emphasis added.

3.2.4 African jurisdictions

3.2.4.1 Free trade agreements with non-African countries

Insofar as African jurisdictions are concerned, there are only three FTAs with non-African countries that mention issues that relate distantly to cross-border data flows, two of which merely touch on it broadly. The 2012 EU-Eastern and Southern Africa States Interim Economic Partnership Agreement (EU-Eastern and Southern Africa Interim EPA) includes ICT policy, infrastructure, and services in the development cooperation areas,[133] while the EU-Ghana economic partnership agreement of 2016 (EU-Ghana EPA) merely stipulates that the parties endeavour to facilitate the conclusion of a global economic partnership agreement with West Africa, which should cover, among others, electronic commerce.[134]

The 2004 US-Morocco FTA includes a provision on 'digital products by electronic transmission' in chapter 14. Problematic terminology aside,[135] regulation 14.3(1) stipulates that the parties do not apply custom duties for the content of such 'products' and agree in paragraph 3 to base the customs value on the value of the carrier medium, without regards to the actual value of the stored content.[136] It mirrors the recently extended WTO Moratorium on Customs Duties on Electronic Transmissions.[137] While one could argue that this and the guarantee of according each other national treatment reflects the US's free-flow-of-cross-border-data approach, it is likely that, at the time, the parties had only traditional physical products in mind, which are convertible into intangible subjects of digital trade without changing its content and much of its value (e.g., physical books vis-à-vis e-books; a movie on a DVD vis-à-vis as data files downloaded via the internet). In relation to a general approach in African jurisdictions, this FTA does not, therefore, allow us to draw any conclusions of substance. The only other relevant FTA is the US-Kenya FTA. Given that it is still

[133] See EU Eastern and Southern Africa Interim EPA, especially Articles 38 and 48.
[134] EU-Ghana EPA, Article 44(a).
[135] While the term 'digital product' is often used, the word 'digital' indicates that the subject traded consists of signals or data expressed as series of the digits 0 and 1 and is thus intangible as opposed to products / goods that are tangible.
[136] US-Morocco FTA, Article 14.3(3).
[137] WTO Ministerial Decision on the Work Programme on Electronic Commerce adopted on 17 June 2022 (WTO document WT/MIN(22)/32 / WT/L/1143).

being negotiated, FTA practice in relation to cross-border data flow regulation does not really exist in African jurisdictions yet.

3.2.4.2 African regional level

The Supplementary Act on Personal Data Protection (2010) within the Economic Community of West African States (**ECOWAS**) to the ECOWAS Treaty (**ECOWAS Supplementary Act**) is the only binding African regional agreement on data protection.[138] It stipulates what content ECOWAS member states must include in their national data privacy laws.[139] It also requires the establishment of a data protection authority (**DPA**) that enforces rules in relation to data breaches.[140] The Southern African Development Community (**SADC**) Model Law on data protection (**SADC Model Law**) establishes principles of data processing, including data minimisation, accuracy, storage limitations, lawfulness and fairness, purpose limitation and accountability.[141]

Once in force, the 2014 Malabo Convention may be of relevance.[142] It would, amongst other things, oblige the AU Members that have ratified it to establish DPAs and observe certain minimum standards, for example in relation to consumer and data protection, as well as cybersecurity.[143] It would also aim for African DPAs to set up cooperation mechanisms among themselves and with others, but without formally requiring the establishment of a mechanism for such cooperation.[144] While 17 of the 32 countries with privacy laws address the establishment of a DPA, failure to constitute them in due time is a common problem.[145] Those that are appointed, moreover, face

[138] Graham Greenleaf and Bertil Cottier, 'International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis' (2022) 44 Computer Law & Security Review 1, 14–15.
[139] For an overview in this regard, see Greenleaf and Cottier (n 140) 21–22.
[140] See ECOWAS Supplementary Act, Chapter IV, especially Articles 14, 19 and 20.
[141] Karishma Banga, Jamie Macleod and Max Mendez-Parra, 'Digital Trade Provisions in the AfCFTA: What Can We Learn From South-South Trade Agreements?' (ODI Supporting Economic transformation (SET) working paper series 2021) 15 <https://bit.ly/3qNampH> accessed 18 September 2022.
[142] Fifteen signatures are required for its entry into force (see Malabo Convention, Article 36). As of March 2022, only 13 countries had ratified the convention: Angola, Cap Verde, Congo, Ghana, Guinea, Mozambique, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, and Zambia <https://bit.ly/3xwfCBU> accessed 17 September 2022.
[143] See Malabo Convention, Articles 11(1)(a), 25(2) and 27(1).
[144] See Malabo Convention, Article 28.
[145] Banga, Macleod and Mendez-Parra (n 143) 13.

challenges related to their independence, but also financial constraints and a lack of institutional capacity.[146]

Furthermore, Article 14(6)(a) would prohibit the transfer of personal data to a non-member state unless 'the [non-member] state ensures an adequate level of protection of privacy, freedom, and fundamental rights of persons whose data are being or are likely to be processed'. In this context, incorporation of the AU Convention into domestic law might not only harmonise standards relating to data protection and privacy frameworks across African countries but facilitate freer cross-border data flows. For example, the KDPA Regulations refers to the ratification of the AU Convention as one way in which to confirm the existence of appropriate data protection safeguards envisioned in section 49(1) of the KDPA and the KDPA Regulations.

The AfCFTA does not yet include any specific provisions on cross-border data flows. It merely touches on data protection and privacy when reiterating the general WTO General Agreement on Trade in Services (GATS) exception that GATS commitments shall not prevent signatories from adopting measures in relation to national laws on data protection and privacy.[147] Importantly, in February 2020, African Union Heads of State and Government Assembly mandated the State Parties to the AfCFTA to commence negotiations on an e-commerce protocol (AfCFTA Protocol on Digital Trade), which would form part of the third phase of AfCFTA negotiations.[148] In December 2020, its negotiation was said to be fast tracked with the stated aim of finalising negotiations by the end of 2021.[149] This deadline was subsequently extended to September 2022.[150] It is unlikely that this aim is capable of being / will be achieved.

4 Regulatory, institutional, and other challenges

[146] See, for example, Ilori (n 91).
[147] See Article 15(c)(ii) of the AfCFTA Protocol on Trade in Services.
[148] See AU Decision on the African Continental Free Trade Area (AfCFTA) of 10 February 2020 (Doc. Assembly/AU/4(XXXIII)) <https://bit.ly/3BYHr8R> accessed 18 September 2022.
[149] See AU Decision on the Start of Trading under the African Continental Free Trade Area (AfCFTA) of 5 December 2020 (Doc. Ext/Assembly/AU/Decl.1(XIII)) <https://bit.ly/3QRu7Hp> accessed 18 September 2022.
[150] See AU Decision on the African Continental Free Trade Area (AfCFTA) of 6 February 2022 (Doc. Assembly/AU/Dec. 831(XXXV)) <https://bit.ly/3Lnxh4w> accessed 18 September 2022.

When regulating cross-border data flows, governments face several regulatory, institutional, and other challenges. Perhaps the most prevalent challenge for governments is to balance competing policy goals (discussed in section 4.1). Governments also face difficulties when it comes to policy coordination across different areas of regulation (discussed in section 4.2), experience capacity and budgetary constraints (discussed in section 4.3), and often lack a shared understanding of concepts and legitimate policy goals (discussed in section 4.4).

4.1 Balancing competing policy goals

There are many different economic (discussed in section 4.1.1) and non-economic (discussed in section 4.1.2) rationales for allowing or restricting certain types of data flows. While it is not necessary to determine intent to classify a restriction as trade distortive, i.e., a measure or set of measures that provides a competitive advantage as a factual inquiry, striking a balance between different rationales reflected in what are often competing policy goals is something that essentially all governments seem to find challenging (a conclusion we reach in section 4.1.3).

4.1.1 Economic rationales

The most prevalent economic rationales for allowing or restricting certain types of data flows are, on the one hand, the costs generally associated with trade distortive cross-border data flow restrictions (discussed in section 4.1.1.1) and, on the other, the potential benefits that may flow from an effective digital industrial policy (discussed in section 4.1.1.2).

4.1.1.1 Asserted costs of trade distortive restrictions

The economics of contemporary cross-border data flows is still a novel subject. Little consensus has emerged insofar as terms and conceptual frameworks are concerned, and what empirical work is available is often scant, lacks a consistent methodological approach, or has not been replicated. Put differently, there are many things that we do not know about the economics of cross-border data flows and the discourse is still evolving (albeit quickly). There have, however, been several studies on the economic cost of forms of 'data protectionism' in terms of which 'data protectionism' is equated to what we understand as barriers to digital trade that come in the form of trade

distortive restrictions to cross-border data flows.[151] The results of these studies often favour freer cross-border data flows over trade distortive restrictions, with some of the following results having been obtained:

- → freer cross-border data flows contribute more to increases in GDP than does trade in goods;[152]
- → freer cross-border data flows lead to greater productivity;[153]
- → greater cross-border data flow restrictions mean higher costs for local businesses;[154]
- → cross-border data flow restrictions tend to harm GDP growth;[155]
- → freer cross-border data flows enable growth in all industries (as opposed to only for economic actors whose core business is or relates to data, including mining companies, manufacturers, retailers);[156]
- → restrictions on cross-border data flows raise costs for consumers;[157] and
- → the costs of restrictions on free flows are or will be borne predominantly by smaller businesses, or that smaller businesses stand to benefit disproportionately from freer flows.[158]

Admittedly, these outcomes are very general in nature. We expect the economic cost to differ from restriction to restriction. Internet filtering might be more harmful from an economic perspective than the implementation of data localisation measures in one context, and data localisation measures may be more damaging economically than data protection measures in

[151] See section 2.6 above.
[152] See James Manyika and others, 'Digital Globalization: The New Era of Global Flows' (McKinsey Global Institute 2016) <https://mck.co/3y6Oomi> accessed 18 September 2022.
[153] See Manyika and others (n 156); Ferracane (n 45).
[154] See Manyika and others (n 156); Ferracane (n 45).
[155] See Ferracane (n 45).
[156] See Ferracane (n 45); Daniel Castro and Alan Mcquinn, 'Cross-Border Data Flows Enable Growth in All Industries' (ITIF 2015) <https://bit.ly/3bdNdIp> accessed 18 September 2022.
[157] See, for example, Nigel Cory, 'The False Appeal of Data Nationalism: Why the Value of Data Comes From How It's Used, Not Where It's Stored' (ITIF 2019) <https://bit.ly/3OtIPTY> accessed 18 September 2022.
[158] See, for example, GSMA, 'Cross-Border Data Flows: Realising Benefits and Removing Barriers' (2018) <https://bit.ly/3LuHook> accessed 18 September 2022; Manyika and others (n 156).

another. The extent to which each of these statements is true can only be properly assessed with all relevant information at hand for the specific context. Due to the difficulties associated with measuring the quantity, frequency and effects of data flows, this information is, however, often lacking. Precise predictions are particularly challenging when considering restrictions that are merely prospective in nature and are geared towards bringing about long-term goals.

4.1.1.2 Potential benefits of trade distortive restrictions from a digital industrial policy perspective

Several other studies focus on the extent to which some forms of restriction may be useful from a digital industrial policy perspective,[159] with these studies acting as a counterweight of sorts to some of the negative impacts associated with curtailing the free flow of data across borders. These negative impacts relate to what one might term as 'digital latecomers',[160] and are of particular salience against the backdrop of international inequalities that we discuss below in section 5.3.2.1 in detail. At the same time, cross-border data flows enable digital MNEs to service foreign markets without really establishing a presence in those markets. Therefore, and unlike traditional MNEs, digital MNEs have asset light foreign investment footprints.[161] This means that there is little to gain for digital late comers, or at least far less than in sectors with lower levels of digital intensity, in the form of inward foreign direct investment (FDI) by foreign digital MNEs. While industrial policy mechanisms such as data localisation requirements or taxation of data flows employed to establish or strengthen a domestic digital industry have been prominently applied by China, to date these measures remain fragmented and the extent of their effectiveness for establishing domestic digital industries elsewhere is far from certain.[162]

[159] See, for example, Christopher Foster and Shamel Azmeh, 'Latecomer Economies and National Digital Policy: An Industrial Policy Perspective' (2020) 56 The Journal of Development Studies 1247.
[160] See, for example, Foster and Azmeh (n 163).
[161] See, for example, Bruno Casella and Lorenzo Formenti, 'FDI in the Digital Economy: A Shift to Asset-Light International Footprints' (2018) 25 Transnational Corporations 31.
[162] Foster and Azmeh (n 163) 1248.

4.1.2 Non-economic rationales

There are also non-economic rationales for restricting cross-border data flows under certain circumstances. One of the main goals governments have in this regard today is the protection of privacy (discussed in section 4.1.2.1), but there are also various other public policy goals that governments pursue (some of which are discussed in section 4.1.2.2).

4.1.2.1 Privacy protection

It is a 'fact of modern life' that 'unless you're willing to live completely off-the-grid, someone, somewhere is compiling a profile of you'.[163] More specifically:

> Even if you are one of those people who eschews social media and resists the temptation to document your life online, you can't escape the big data gobblers that have insinuated themselves into every aspect of our lives. Companies across all industries are using technology to collect data on you. Think about it:
>
> Your smartphone continuously tracks your whereabouts. Beyond that, your service provider can access all the information you have stored on your device, including your contacts' information and how often you receive or send a text.
>
> Smart grids track your energy usage and collect details about your life — from your daily routines to the appliances you use.
>
> Insurance providers will offer you a discount if you let them track your every move while driving.
>
> The healthcare industry is pushing for devices that would allow doctors' to collect data on you outside of the doctor's office. For example, Apple recently launched its HealthKit platform, which allows doctors to collect real-time data from iPhones and Apple devices.
>
> Companies, using browser fingerprinting, cookies, authenticated tracking, cross-device tracking and other methods, are monitoring your online activity and using that data to send you targeted ads.

[163] Daniel Burrus, 'The Privacy Revolt: The Growing Demand For Privacy-as-a-Service' [2015] *Wired* <https://www.wired.com/insights/2015/03/privacy-revolt-growing-demand-privacy-service/> accessed 18 September 2022.

> Those are just a handful of ways you are being tracked.[164]

Constant tracking and profiling have led to, amongst other things, the concept of 'surveillance capitalism' gaining traction in both academic and non-academic life. It refers to 'the unilateral claiming of private human experience as free raw material for translation into [behavioural] data'.[165] According to Shoshana Zuboff, for example, '[t]hese data are then computed and packaged as prediction products and sold into [behavioural] futures markets — business customers with a commercial interest in knowing what we will do now, soon, and later'.[166] She further asserts that '[a]t its core, surveillance capitalism is parasitic and self-referential' and that it 'revives Karl Marx's old image of capitalism as a vampire that feeds on [labour], but with an unexpected turn [–] Instead of [labour], surveillance capitalism feeds on every aspect of every human's experience'.[167] If one subscribes to this view, or even to a less strongly worded version of it, the prediction of what might be termed a 'privacy revolt' does not seem so far-fetched. However, given that there is often a 'general disconnect between consumers' self-stated privacy preferences and their actual privacy-seeking [behaviour]',[168] it is disputable whether a 'revolt' worthy of the term has in fact taken place. While consumers may say they value privacy in the digital world, they often share their personal data quite extensively.[169] This might be termed the 'privacy paradox'.[170]

Regardless of whether one subscribes to a version of surveillance capitalism or focuses on the extent to which people are willing to share their data voluntarily, the demand for more privacy protection in the digital economy has risen, particularly in relation to personal data. While data protection laws aim, at least rhetorically, to meet this demand, they increasingly restrict data flows,

---

[164] Burrus (n 167).
[165] John Laidler, 'High Tech Is Watching You' <https://bit.ly/2HokizY> accessed 18 June 2022.
[166] Laidler (n 169).
[167] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019) 9.
[168] See, for example, Long Chen and others, 'The Data Privacy Paradox and Digital Demand' (NBER Working Paper 2022) 1 <http://wxiong.mycpanel.princeton.edu/papers/Privacy_Paradox.pdf> accessed 18 June 2022.
[169] For a useful summary of evidence on this score, see Alessandro Acquisti, Laura Brandimarte and George Loewenstein, 'Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age' (2020) 30 Journal of Consumer Psychology 736.
[170] See, for example, Chen and others (n 172).

and cross-border data flows in particular. In countries where privacy is protected as a fundamental right within a constitutional or similar framework, but also in all places where online privacy is valued and governments are at least somewhat responsive to what their citizens value, such restrictions are easy to justify. Since data flow restrictions seem to come, as illustrated above,[171] with certain economic costs, the extent of such restrictions based on privacy grounds implies that certain trade-offs must be made, and balances struck.

The extent to which people are willing to share their data voluntarily may play a decisive role when deciding what constitutes an optimal level of data protection. The meaning of the word 'voluntarily' might also need to be assessed in context. Many digital MNEs essentially collect and sell data and, as such, 'provide free services to netizens in return for the use of their personal data (e.g. Google search and Facebook's social network)', the idea in this model being that 'individuals [might] not understand or recognize their responsibility for internet security and stability'.[172] This 'tragedy of commons' might require more intervention to protect the safety and privacy of users (netizens).[173]

4.1.2.2 Other non-economic public policy goals

Other non-economic rationales for restricting cross-border data flows include food safety, health concerns and consumer protection.[174] Moreover, several governments, for example Kenya and South Africa, contemplate imposing data localisation measures to assist with providing national security agencies with access to data for law enforcement reasons. Some governments, for example China and Russia, limit cross-border data flows for purposes of censorship and general surveillance of their citizenry.[175] This might destabilise parts of the internet or reduce its openness,

---

[171] See section 4.1.1 above.

[172] Aaronson, 'What Are We Talking about When We Talk about Digital Protectionism?' (n 10) 547.

[173] Bill Davidow, 'The Tragedy of the Internet Commons' [2012] *The Atlantic* <https://bit.ly/3dlORJH> accessed 17 September 2022.

[174] At the WTO level, these are partly reflected in technical barriers to trade and sanitary and phytosanitary rules and standards.

[175] For a discussion in this regard, see, for example, Centre for IT and IP Law, KU Leuven, 'Government Access to Data in Third Countries' (Final Report EDPS/2019/02-13, 2021) <https://bit.ly/3RUUuxl> accessed 18 September 2022. See

impede access to information, disrupt communication, or undermine human rights (freedom of expression) and scientific progress. Some filtering measures such as 'take down' requirements might, however, be aimed at fulfilling the so-called right to be forgotten (to the extent that it is recognised in a given jurisdiction),[176] or at protecting IP rights.[177]

4.1.3 The need for balancing competing priorities, interests, and public policy goals

Putting aside that priorities, interests, and public policy goals differ from country to country, there is no clear model that policymakers would be able to use to distinguish between legitimate and illegitimate cross-border data flow regulation. Moreover, at an empirical level, it is difficult to assess what impact certain policies will have given that there are very few data on cross-border data flows available. For example, adopting data localisation requirements aimed at protecting cyber-security would assume that data stored on local servers is more secure from hackers and the like than data stored elsewhere. Such an assumption (or claim) is hard to validate without an empirical determination. More so, if one considers that some countries are more technologically advanced vis-à-vis other countries when it comes to securing data, then the 'other' countries might be better off, from a cybersecurity perspective at least, if data is stored abroad.[178] However, the benefits (supposedly) associated with localisation measures aimed at encouraging foreign firms to set up data centres or processing operations locally to catch up as a digital late comer might outweigh (i) increased compliance costs, and/or (ii) the desire to ensure that firms can access and process the data of citizens in other countries without hinderance or use foreign firms to provide services for data processing.

---

also Nigel Cory and Luke Dascoli, 'How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them' (ITIF 2021) <https://bit.ly/3RUUz47> accessed 18 September 2022.

[176] Much of the jurisprudence in this regard stems from the EU, where the right is more correctly referred to as the 'right to erasure', and stems from Article 17 of the GDPR. For a good overview of the right to be forgotten / the right to erasure in the EU context, see generally Jure Globocnik, 'The Right to Be Forgotten Is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17)' (2020) 69 GRUR International 380.

[177] For a discussion on this in the EU context, see Oleksandr Bulayenko and others, 'Cross Border Enforcement of Intellectual Property Rights in the EU' (Study for Policy Department for Citizens' Rights and Constitutional Affairs Directorate-General for Internal Policies, European Parliament, PE 703387, 2021) <https://bit.ly/3BTGpuB> accessed 20 September 2022.

[178] For an argument that data localisation actually undermines cybersecurity, see Cory and Dascoli (n 179) 5–6.

This illustrates the need to evaluate on a case-by-case basis the extent to which policy goals actually compete with one another. Moreover, even if a government is able to determine whether public policy goals truly compete with one another, balancing them remains an arduous task, particularly given the fast-moving pace of technological change, the ever-changing dynamics of the demands of citizens or netizens, and the competition between different service providers. That said, regardless of the substance of a given cross-border data flow restriction, if it limits the exchange of the subjects of digital trade covered under the scope of one of the current WTO agreements, WTO law applies concurrently when assessing its legitimacy.

4.2 Policy coordination

Another challenge is policy coordination among different parts of government or, when considering the EU, among different departments of the European Commission. The striking of an appropriate balance among the different policy rationales for allowing or limiting cross-border data flows ideally involves all responsible departments. It likely implicates the departments responsible for international trade, competition, data protection, cybersecurity, law enforcement and IP enforcement, but might affect other departments too, depending on the particular rationale. More so, once a balance is struck, to achieve the overall goals, all implicated departments must take co-ordinated action. This might prove difficult given that some of the implicated departments are primarily tasked with ensuring the attainment of *non-economic* goals and some with securing economic goals.

4.3 Capacity and budgetary constraints

A related problem is capacity constraints. Effective coordination across government departments, entities and agencies requires that all actors involved have a sufficient appreciation not only for the issues arising within their own policy domain, but for the issues arising in all affected policy domains. This calls for investment in human capital, which in light of budgetary constraints, particularly in poorer countries, poses a challenge that is exacerbated by the general inability of regulation to keep pace with rapid technological change. Beyond effective cooperation, the

budgetary constraints in many African countries also result in insufficient enforcement capacity more generally.

4.4 Lack of shared understanding of concepts and policy goals

While all the previously described challenges apply to regulation at the international level as well, additional challenges do arise, chief among which is the lack of a shared understanding in relation to (i) what constitutes a trade distorting restriction to cross-border data flows, (ii) when should such restrictions be permitted, and (iii) why should they be permitted. For example, different countries have different views about the extent to which trade distortive restrictions to cross-border data flows should be permitted to protect privacy. This question arises at both conceptual and practical levels.

At a conceptual level, while some countries take a rights-based approach to privacy protection, others do not. Among those who do take a rights-based approach, there are differences about the scope of the right, as well as in relation to what extent the right can be limited in pursuit of other objectives (and even other rights, including economic and social rights, or developmental rights). This leads to the question: to what extent should economic discrimination be permitted in relation to cross-border data flows or when is a trade distortive restriction legitimate, and when is it illegitimate? The massive difference in approach between the US and China alone illustrates how far away we are, globally, from a shared understanding on the extent to which restrictions of flows should be allowed for economic ends.

At a practical level, views in relation to how best to give effect to privacy protection also differ, regardless of how 'privacy' is defined or whether it is protected as a fundamental right or not. An example is the debate about the extent to which data localisation measures, whether *de jure* or *de facto*, are practically capable of protecting privacy.[179] Another example stems from the discussions about which service providers in which countries are, in reality, 'better' at protecting

[179] See, for example, Svantesson (n 38) 22–23.

privacy.[180] These differing views further relate to questions about jurisdiction, including the extent to which foreign service providers can be sanctioned for failures to protect privacy in foreign countries.[181] Disagreements also exist in relation to the extent to which different people in different countries (i.e., across and within countries) value privacy,[182] and the extent to which they are willing to trade away their privacy for other things.[183]

Since we are very far from reaching consensus on any of these questions and bearing in mind that there is significant divergence on the extent to which trade distortive restrictions are costly or beneficial,[184] concluding an agreement that serves all involved countries' interests (never mind diverging interests within those countries) is very difficult. Hence, it is challenging, to say the least, to meaningfully regulate cross-border data flows in FTAs, particularly given the strong propensity that measures imposed to protect privacy or achieve other public policy goals have to affect cross-border data flows and, therefore, digital trade. Also noteworthy here is that most governments have not yet ascertained (i) whether and to what extent to regulate data analytics, artificial intelligence (AI), and other new technologies that rely heavily on personal data,[185] (ii) whether and to what extent to contest the monopoly power of large technology firms (so-called Big Techs) and (iii) how to address the opacity of the algorithms used by many platforms.

[180] See Svantesson (n 38) 22–23.
[181] See, for example, Svantesson (n 38) 16–17.
[182] See, for example, Yao Li, 'Cross-Cultural Privacy Differences' in Bart P Knijnenburg and others (eds), *Modern Socio-Technical Perspectives on Privacy* (Springer International Publishing 2022).
[183] See, for example, Jeffrey Prince and Scott Wallsten, 'Empirical Evidence of the Value of Privacy' (2021) 12 Journal of European Competition Law & Practice 648.
[184] See section 4.1.1.
[185] See, for example, Taylor Owen, 'Ungoverned Space: How Surveillance Capitalism and AI Undermine Democracy' (Centre for International Governance Innovation) <https://bit.ly/3UiiHzc> accessed 17 September 2022; United Nations Conference on Trade and Development, 'Cyberlaws and Regulations for Enhancing E-Commerce: Case Studies and Lessons Learned' (Note by the UNCTAD secretariat, Doc TD/B/CII/EM5/2, 2015) <https://bit.ly/3DE1muZ> accessed 18 September 2022. Many countries do, however, have e-transaction, consumer protection, privacy, and cybercrime laws in place to facilitate an appropriate enabling environment.

5 Policy recommendations

With all the discussed approaches and challenges in mind, our recommendation is to approach the regulation of cross-border data flows in Africa in a chronological fashion (discussed in section 5.1). We then continue by pointing to what is needed to determine whether establishing rules on cross-border data flows under the AfCFTA is currently a worthwhile pursuit (in section 5.2). We then recommend several factors which we believe must be specifically considered when deciding on the approach towards trade distortive restrictions vis-à-vis allowing data to flow freely across borders when attempting to accommodate the peculiarities of Africa (in section 5.3). Thereafter, we briefly discuss policy coordination (in section 5.4) and conclude with a discussion on what issues need to be decided on when establishing rules on cross-border data flows (in section 5.5).

5.1 On a chronological approach: taking time to get things right

We begin by recommending that AfCFTA State Parties take their time to get things right, and that a chronological approach be adopted to regulation, i.e., countries should first set national priorities and formulate their own comprehensive data flow strategies and legislative frameworks in accordance with these priorities before concluding FTAs that include provisions regulating cross-border data flows. This recommendation starts from the premise that much can be achieved at the domestic level when it comes to regulating cross-border data flows. Moreover, once national priorities and strategies are in place, FTAs can subsequently be concluded with a view to supporting these priorities and strategies – national priorities and strategies are then able to guide a given country in its negotiations with others. If these steps are reversed, i.e., FTAs are concluded first, the ability of State Parties to subsequently set national strategies would be constrained by their international obligations, which will be difficult to unwind at a later stage. Thus, a chronological approach would allow African countries to conclude FTAs that are consistent with their respective national legislations and policies. Since most African countries have yet to conclude FTAs that include (extensive) provisions regulating cross-border data flows, there is still room for taking a chronological approach.

5.2 On what is needed to determine whether rules on cross-border data flows under the AfCFTA are worthwhile pursuing

5.2.1 Shared understanding of concepts and terminology

Prior to any attempts to pursue a set of rules regulating cross-border data flows in the AfCFTA Protocol on Digital Trade, AfCFTA State Parties would have to clarify whether and to what extent they share an understanding of the substance of the various relevant concepts and terminology involved in the regulation of cross-border data flows such as digital trade, e-commerce, data, trade barriers to digitally enabled trade, cross-border data flows, and data protectionism, amongst numerous others.[186] This includes identifying whether and to what extent they share a conceptual understanding on how these terms relate to each other specifically within the realm of cross-border data flow regulation. If State Parties' understanding of terminology differs, the quality of negotiations will be impaired because the negotiating parties will be talking at cross-purposes.

5.2.2 Shared norms, values, and policy goals

Provided that there is a shared understanding on terminology, AfCFTA State Parties would next need to determine whether and to what extent they share norms, values and policy goals in relation to the issues implicated in regulating cross-border data flows (e.g., privacy protection, consumer protection, socio-economic rights, the right to development, national security, access to information, freedom of science, freedom of expression, cybersecurity abd bridging digital divides). The process of determining whether and to what extent the parties share (i) an understanding of terminology and (ii) norms, values and policy goals would contribute to all parties having clarity on and comprehension of the issues involved when regulating cross-border data flows. The more State Parties' norms, values, and policy goals align, the more likely they are reconcilable in negotiations.

[186] For an overview of our understanding and suggestions in this regard, see section 2 above.

5.2.3 Shared theoretical and practical understanding of the aims of potential rules on cross-border data flows

If AfCFTA State Parties really do have norms, values, and policy goals that sufficiently align, they would then have to determine whether and to what extent they share an understanding of (i) what potential AfCFTA rules on cross-border data flows should achieve in theory, and (ii) how they will achieve these theoretical aims in practice. Most importantly, this includes a shared understanding – ideally based on shared norms, values, and policy goals – of the extent to which trade distortive restrictions to cross-border data flows should be permitted in relation to both economic and non-economic policy goals. The greater the alignment of State Parties' understanding of how much control over, and restrictions of cross-border data flows is deemed legitimate, the more likely it becomes that negotiations will yield effective and legitimate rules.

5.3 On what to consider when deciding on the approach towards restrictions vis-à-vis free flow of cross-border data

Assuming State Parties are reasonably aligned on what constitutes legitimate regulation, they will then need to agree on a more specific approach towards trade distortive restrictions vis-à-vis free flow of cross-border data and attempt to strike a concrete balance between economic (discussed in section 5.3.2) and non-economic (discussed in section 5.3.3) rationales and policy goals. To accommodate the peculiarities of African countries, we provide recommendations on what must be considered when deciding on such an approach. We start by drawing attention to the urgent need for the kind of data collection that will enable evidence-based rule making by the State Parties (in section 5.3.1) and then end by recommending that the regulation of cross-border data flows be approached holistically (in section 5.3.4).

5.3.1 Data collection for evidence-based rules and policy making

We recommend that negotiating parties pursue evidence-based rules and policy making. This starts by not relying on one of the many unfounded and interest-driven general economic claims on the potential impacts (i.e., benefits and costs) of trade distortive restrictions vis-à-vis the free flow of data that predominantly or exclusively benefit certain actors without proper consideration

of others. Admittedly, however, it is difficult to identify good faith attempts to quantify and explain the economics of cross-border data flows. As such, we urge negotiators to treat economic claims in relation to the impact of restrictions on cross-border data flows (sometimes equated with data protectionism) with a healthy level of scepticism. In this still (quickly) evolving discourse, there are many things we simply do not know yet. Thus, whenever negotiators evaluate a particular economic claim, we strongly recommend inquiring who benefits from the acceptance of a claim and actions taken in accordance with that claim. In addition, there is not only a general lack of widely accepted research on the economics of cross-border data flows, but the vast majority of the relatively small number of existing studies speak to contexts applicable elsewhere (often in developed countries or large economies in different parts of Asia), and not to African contexts. As such, negotiators must be cautious when referring to them as holding true on the continent. Moreover, while rules on cross-border data flows in agreements concluded elsewhere in the world can provide guidance and inspiration on how to address certain issues, these agreements differ largely in their respective approaches,[187] and often relate to very different circumstances than those existing in African countries.

In the absence of proper evidence, reliable and comprehensive Africa-specific data is needed to adequately assess the economic benefits and drawbacks of restrictions on cross-border data flows in the African context. This data, however, will, once available, only be the starting point for the rigorous further research necessary to answer questions on these important topics. Such data and research would provide a better basis for negotiators to familiarise themselves with the implications of possible approaches and, therefore, allow evidence-based rules and policy-making when drawing conclusions on whether, on balance, certain approaches are in fact beneficial to domestic over foreign firms. This could include 'sequencing' around national digital policy, i.e., analysing the dynamics of digital industrialisation to gain an understanding when and under what

[187] See above section 3.

conditions different types of policy levels might be used. Such 'sequencing' could provide industrial policy directions for individual African countries, and indeed the continent as a whole.[188]

Notably, however, much of the desired evidence will only become available through policy experimentation. To ensure that course correction is possible if a particular course of action is not working when countries engage in trial and error, proper feedback mechanisms must be put in place. This point also further reinforces the importance of taking a chronological approach and not rushing to conclude rules at the international level.

5.3.2 Africa-specific economic rationales

Generally, as mentioned above, there is evidence suggesting that the fewer restrictions to cross-border data flows are adopted, the more potential there is for economic growth.[189] However, these outcomes and economic claims are very general in nature and focus on different contexts, usually those of developed countries or large Asian economies. Since potential growth and asserted costs might not materialise in the same manner for all, these outcomes must be viewed from a distributional perspective, that is, it must be carefully determined who benefits from what types of regulation. Seen this way, it is first necessary to understand divides and inequalities in accessing the digital world and in taking advantage of the opportunities offered by the data economy (discussed in section 5.3.2.1) before thinking about how best to navigate distributional issues and the consequences thereof when regulating cross-border data flows (discussed in section 5.3.2.2).

5.3.2.1 Digital divides and inequalities

A comprehensive discussion of economic, digital and data divides and inequalities both in accessing the digital world and in taking advantage of the opportunities offered by the digital and data economies goes beyond the scope of this report. It is therefore not our intention to be exhaustive, but merely to provide a sense of the issues at stake. While there are many ways of

[188] See Foster and Azmeh (n 163) 1258.
[189] See above section 4.1.1.

describing levels of digital inequalities, in accordance with 'core, long standing tropes in digital inequalities research',[190] we differentiate between three levels, that is in relation to: (i) digital access; (ii) usage; and (iii) benefits / outcomes.[191] The three levels are hierarchical and linear but intertwined. To benefit from data flows, one must first have access to data flows. Since data usually flows digitally via the internet, this is about access to the internet. Without such access, data cannot be used, and, in turn, benefits cannot accrue. Moreover, having access to data does not mean that one necessarily possesses the requisite skills to in fact do so. Equally, even if access is available, one does not automatically move to the next level, which means being able to use the data. Usage, too, requires skills, which might initially be lacking. While it further remains uncertain whether one ultimately benefits, access and usage certainly increase the chances of benefitting.

A closer look at access inequalities reveals that only about half of the world's population accesses and uses the internet,[192] with significant gaps between countries. In developed countries, nearly 87 percent of people have access to the internet as compared to 47 percent in developing countries and 19 percent in least-developed countries (LDCs).[193] Given that the majority of LDCs are in Africa, it is no surprise that large portions of the various national populations on the continent are still offline and, thus, excluded from the digital and data economies. This is mainly due to the costs associated with access, underdeveloped ICT infrastructure and overall low levels of technological literacy, all of which are closely correlated to geography and socio-economic status.[194]

---

[190] Jonathan Cinnamon, 'Data Inequalities and Why They Matter for Development' (2020) 26 Information Technology for Development 214, 227. There is also the 'mirror trope', i.e., inequalities 'reflect extant social and structural inequalities' and the 'poverty trope', i.e., the idea that data 'haves' and 'have nots' are determined by the accumulation of factors accrued at societal, community, and individual scales.

[191] Shin-yi Peng refers to the idea of a 'network layer' as opposed 'access'. See Shin-yi Peng, 'The Uneasy Interplay between Digital Inequality and International Economic Law' (2022) 33 European Journal of International Law 205, 208–210.

[192] International Telecommunication Union, 'Most of the Offline Population Lives in Least Developed Countries' <https://bit.ly/3ROErkG> accessed 17 September 2022.

[193] International Telecommunication Union (n 196).

[194] See, for example, United Nations Conference on Trade and Development, 'UNCTAD Rapid ETrade Readiness Assessments of Least Developed Countries: Policy Impact and Way Forward' (2019) <https://bit.ly/3QR3kLs> accessed 18 September 2022.

To illustrate the point, in 2022, the majority of Sub-Saharan countries have costs far in excess to the global average, with all but 12 of the 44 countries in the region sitting in the most expensive half of the 220 compared countries in a recent study.[195] Burundi charges residential users an average of $430 per month for fixed-line broadband, which is estimated to be the most expensive in the world, followed by Sierra Leone ($317). Benin joins as one of the most expensive countries in the region ($170), and all sit among the 10 most expensive countries in the world. In some African countries, information on prices available is not even available (e.g., Central African Republic, Chad, Congo, Guinea, and the territory of Western Sahara). Given that the average monthly income in many African countries is lower than the average monthly broadband cost, it is no surprise that internet penetration is very low in these countries. The picture is even worse when it comes to the average broadband speed, with most of the slowest countries being on the African continent.[196] This explains the limited connectivity in many African countries, particularly in rural areas as compared to urban areas and why, in general, LDCs lag behind most other countries in digital readiness.[197]

Moving beyond mere internet access, in 2020, 89 percent of all North Americans were connected to the internet via at least 3G wireless broadband technology, whereas the corresponding figure for Sub-Saharan Africa was 22 percent.[198] Similarly, mobile data consumption varies substantially by country income group. In 2018, in high-income countries, monthly per capita mobile data consumption stood at around 7.1 gigabytes (GB), whereas the corresponding figures in lower-middle- and low-income countries were 1.3 and 0.2 GB respectively.[199]

---

[195] Dan Howdle, 'Worldwide Broadband Price Research 2022' (cable.co.uk) <https://bit.ly/3QTAdai> accessed 17 September 2022.

[196] Dan Howdle, 'Worldwide Broadband Speed League 2022' (cable.co.uk) <https://bit.ly/2F1cF1s> accessed 18 September 2022.

[197] See, for example, United Nations Conference on Trade and Development, 'The Least Developed Countries in the Post-COVID World: Learning from 50 Years of Experience' (United Nations 2021); *The Least Developed Countries Report 2020: Productive Capacities for the New Decade* (United Nations 2020).

[198] See World Bank (n 24) 161.

[199] See World Bank (n 24) 166.

With the Fourth Industrial Revolution (4IR) being upon us, the extent of current access disparities seems likely to increase. First, the 4IR might exacerbate digital divides because 4IR technologies will increasingly be propelled by the recent uptake of 5G network technology. The deployment thereof requires such high levels of investments that the ITU predicts that 5G penetration will be around 59 percent in developed economies by 2025, whereas the same network connectivity during the same period will be around 8 percent in Latin America and 3 percent in African countries.[200] Second, the 4IR might increase economic divides because one of its core aims is to connect machinery.[201] The concern is that

> smart manufacturing enterprises operates more like software companies, requiring employees to design, program, operate, and debug 'smart' machines. That know-how will more likely reside in a few leading countries, with the United States, Europe, China, and a few others vying for leadership.[202]

This could lead to so-called pre-mature de-industrialisation for developing countries that are still trying to catch up economically through industrialisation. On the one hand, such de-industrialisation might '[trap] them at low-income levels in services sectors',[203] whereas, on the other, rising labour costs elsewhere could ostensibly enable labour-abundant African countries to ramp up exports of low-value manufactures and services and better integrate into global value chains.

Digital access disparities exist not only between African countries/regions and the world, but among African countries. Notably, nowhere else is the digital divide starker than in Africa, with ICT development moving at a globally competitive pace in Cairo, Nairobi, Lagos, and Cape Town.[204]

---

[200] United Nations Conference on Trade and Development, *Value Creation and Capture: Implications for Developing Countries (Digital Economy Report 2019)* (United Nations 2019) 7.

[201] This includes technologies such as 3D printing, the Internet of Things (IoT), AI and the various (other) technologies underpinning big data analytics.

[202] See Shaffer (n 51) 266.

[203] Shaffer (n 51) 266.

[204] Franziska Sucker, 'COVID-19 Pushes Digital Solutions and Deepens Digital Divides: What Role for African Digital Trade Law?' <https://bit.ly/3QQtpdp> accessed 17 September 2022.

There are also disparities within countries, with them being significant in those countries where globally competitive firms are located and possibly linked to stark income inequalities.

Considering the case of South Africa, one observes that approximately 32 percent of South African residents in the ZAR 0–1 583 income group (i.e. people who earn up to approximately $100 per month) and about 10 percent of South Africans in the ZAR 1 584–7 167 income group (i.e., monthly income of between approximately $100 and $450 per month) did not have access to the internet at all by 2018.[205] In all other income groups, 100 percent of residents had access to the internet.[206] The fact that approximately 90 percent of South Africans earn less than ZAR 7 167 per month and more than 60 percent of South Africans earn less than ZAR 1 584 per month illustrates the significance of this gap.[207] These statistics speak purely to access and do not account for disparities in usage, which are naturally far higher.

These examples only begin to illustrate how the extent to which one is able to benefit from data flows is related, among other reasons, to which country or region one finds oneself in, and where in the economic spectrum one finds oneself within that country or region. To put this into context, when adjusting for purchasing power, World Bank calculations for 2020 reveal that per capita GDP for Sub-Saharan African countries on average is approximately $3 900 or approximately 16 times less than the almost $61 500 figure for North Americans in the same year.[208] This still masks the vast economic inequalities within many countries, as our South African example above demonstrates.[209]

Existent digital access inequalities penetrate all the way to the benefit and outcome level. Ninety percent of large-scale digital platforms (Big Techs) are controlled by firms based in the US (e.g., Alphabet (Google), Amazon, Apple, Meta (Facebook), Microsoft, Twitter Netflix, Tesla) or China

---

[205] Alison Gillwald, Onkokame Mothobi and Broc Rademan, 'The State of ICT in South Africa' (Research ICT Africa 2018) 113 <https://bit.ly/3QOCjIl> accessed 18 September 2022.
[206] Gillwald, Mothobi and Rademan (n 209) 113.
[207] See SALDRU, 'Income Comparison Tool' <https://www.saldru.uct.ac.za/income-comparison-tool/> accessed 18 September 2022.
[208] See World Bank, 'GDP per Capita, PPP (Current International $) - Sub-Saharan Africa, North America' <https://bit.ly/3qM6lwp> accessed 18 September 2022.
[209] Note, however, that the South African income group figures are not adjusted for purchasing power.

(e.g., Alibaba, Baidu, Tencent). Digital platforms in African and Latin American countries combined account for only 1 percent.[210] For example, out of 4124 global co-locations, only 6 major data centres are located in East Africa (5 in Kenya, 1 in Tanzania).[211] Thus, not only is a lion's share of digital content in Africa consumed from data which flows to Africa from outside the continent, but African countries are also net data exporters, supplying data for analysis and commoditisation abroad without benefitting.[212]

The large scale and scope of user data collected provides leading global digital platform firms with a competitive advantage that can easily be equated with dominance on a global scale.[213] In addition, the risk of hoarding data and, thus, of expanding data capitalism,[214] may limit potential competitors' entry into future data-driven sectors such as AI. This is likely to widen economic and digital inequalities. Notably, some scholars view Big Techs' appropriation and extraction of data for profit all over the world as 'data colonialism'.[215] Given the highly uneven distribution of benefits and outcomes within data-intensive industries globally, it follows that there are many countries that are still attempting to build domestic data-intensive industries, not to speak of sectors that are well-placed to benefit from the 4IR. These countries are so-called digital late comers, and this set of countries includes most, if not all, African countries.[216]

---

[210] See Antonio Andreoni and Simon Roberts, 'Governing Data and Digital Platforms in Middle Income Countries: Regulations, Competition and Industrial Policies, with Sectoral Case Studies from South Africa' (Oxford Digital Pathways Paper Series, Paper 5, 2020) 18 <https://bit.ly/3BRcT8Y> accessed 18 September 2022. See also communication from India and South Africa, Work Programme on Electronic Commerce, 'The E-commerce Moratorium: Scope and Impact', WT/GC/W789 (10 March 2020), para 3.4 (and the sources relied on there) <https://bit.ly/3Sg1Par> accessed 18 September 2022.

[211] Data Center Map <www.datacentermap.com/> accessed 18 September 2022.

[212] Data Center Map <www.datacentermap.com/> accessed 18 September 2022.

[213] See also Zuboff (n 171).

[214] On the concept, see above Peng (n 195) 224–225.

[215] See Peng (n 195) 213; Nick Couldry and Ulises A Mejias, *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019) 83–85;187–196; Sarah Myers West, 'Data Capitalism: Redefining the Logics of Surveillance and Privacy' (2019) 58 Business & Society 20, 24.

[216] See, for example, Foster and Azmeh (n 163).

5.3.2.2 Navigating distributional inequalities: development-focused industrialisation

As time passes, the myriad distributional inequalities already referred to constitute ever greater challenges.[217] Thus, disparities of the nature described, particularly the fact that most African countries are digital late comers,[218] must be at the forefront when regulating cross-border data flows in Africa.

Brazil, India, Indonesia and especially China are examples of digital late comers that have used cross-border data flows that distort trade as part of their digital industrial policy to develop their domestic technology sectors, support domestic firms and leverage the services offered by international firms in ways that are beneficial to the digital late comers. Some of these sectors are now either globally competitive or service their domestic markets effectively in ways that are consistent with their developmental goals. However, when developing and expanding, most domestic digital firms in these countries tend to focus on developing market power domestically with the support of private (often international) capital.[219] Due to the much smaller domestic markets in African countries, a replication of these emerging countries' journey by employing similar industrial policy mechanisms seems implausible. Simultaneously, it is doubtful that, absent strategic interventions, which entail trade distortive restrictions to cross-border data flows, African countries will be able to develop their own data-intensive, digital industries that could effectively compete domestically and, perhaps even internationally.

It goes beyond the scope of this report to determine the potential benefits and cost of all possible strategic interventions that would counter the fact that

(i) African countries are digital late comers;

[217] On why distributional inequalities matter, see, generally, for example, Thomas Scanlon, *Why Does Inequality Matter?* (Oxford University Press 2018).
[218] Gender, racial and educational inequalities are among a long list of other factors one might consider in their own right, albeit that these inequalities interact in various ways with economic inequality.
[219] Foster and Azmeh (n 163) 1257.

(ii) they operate in a global landscape that already contains massive digital MNEs, most of whom are virtual monopolies (usually based in countries which are significantly richer than African countries);

(iii) huge differences in economic development among African countries remain; and

(iv) different African countries assimilate into the digital and data economies at different rates.

We seek, however, to provide readers with at least a sense of potential suitable development-focused industrialisation measures that would aim to ensure that existing digital and economic divides are not exacerbated, or, in an ideal world, would actively aim at reducing such divides. Therefore, we allude to six aspects that require consideration when approaching the extent to which regulatory intervention is necessary in relation to cross border data flows, while acknowledging that digital inequality levels are, indeed, 'so intertwined that their independent solution might lead to a contradiction'.[220]

5.3.2.2.1 Establishing who benefits from what and how, and who should benefit

To appropriately regulate cross-border data flows against the backdrop of the actual and potential distributional consequences of implementing such regulation, policy- and rule-makers acting in good faith must seek to identify who stands to benefit from prospective and existing regulation and, more importantly, who *should* benefit. Admittedly, this is an incredibly challenging task, as it is hard to anticipate how such regulation will affect African countries' ability, as a whole and as individual countries, to compete with countries outside of Africa (as well as with one another), especially in the absence of Africa-specific data.[221]

What is beyond controversy, though, is that digitally delivered subjects of trade are non-rivalrous (at least conceptually) and replication costs are almost zero.[222] Thus, generally, the freer the flow of cross-border data, the more firms that rely on cross-border data flows for exchanging their products are able to reap the benefits that come with it (including lower search

[220] Peng (n 195) 208.
[221] The collection of which should, as we have already argued above in section 5.3.1, be a priority.
[222] See section 1 above.

costs, lower transportation costs, lower tracking costs, and lower verification costs).[223] Adopting a largely free-flow approach to rule-making in relation to cross-border data flows under the AfCFTA might, therefore, tempt large, dominant digital MNEs to set up their operations in one or two African economies with high technological capacities, which would enable those MNEs to reach the entire African market via regional hubs. The countries with such capacities are likely to be the larger African economies. Ostensibly, countries hosting firms that rely on data flows for exchanging their products may benefit from free data flows serving their constituents (while also facing Big Tech's dominance), potentially at the expense of smaller African economies. This might increase digital divides without contributing to the broad-scale development of domestic digital and data-intensive industries in most of the countries on the continent.

Moreover, who controls the data and where the data is controlled influences the benefits that economic actors and consumers are able to reap from cross-border data flows and digitally enabled trade as well as from the purpose and purview of regulation designed to protect the privacy of individuals in relation to their personal data and other non-economic objectives. We therefore recommend focusing on the various data ownership and control aspects when regulating cross-border data flows. This necessitates not only consideration of levels of data localisation, but also building capacity for data collection, storage, and processing, as well as investing in data centres, which will facilitate the development of domestic digital infrastructure and the industries that require such infrastructure to thrive.

5.3.2.2.2 Regulatory autonomy for graduate industry protection

Considering the nascent state of domestic digital and data-driven industries in African countries, we continue by recommending that State Parties take an active role in shaping sectoral conditions. For example, when sectors grow or are perceived to be of strategic importance, support measures for domestic firms might ensure that they can scale up and that their growth is not inappropriately restricted by (possibly predatory) foreign competitors.[224] This might be achieved through, among

[223] On each of these aspects, see further Goldfarb and Tucker (n 3).
[224] Foster and Azmeh (n 163) 1258. This is also known as 'infant industry' protection.

other things, internet filtering, data localisation and frameworks which disrupt … the business models of foreign firms'.[225] Notably, '[g]iven malleable digital technologies and the mobility of knowledge around digital technologies, state-induced linkages and technology transfer appear less important to early firm expansion'.[226] To be able to adopt such measures and formulate their domestic trade policies in a way that would allow them to reduce poverty, industrialise and integrate into the global digital trading system, State Parties must retain sufficient regulatory autonomy. This, too, is in accordance with our recommendation to adopt a chronological approach to the AfCFTA Protocol on Digital Trade rule making.[227]

5.3.2.2.3 Regulatory autonomy for reducing inequality within the territories of State Parties

State Parties retain responsibility for addressing and responding to their own distributional challenges through, for example, competition regulation,[228] taxation,[229] and social security policies.[230] Nonetheless, it is in the interest of each State Party that distributional inequalities in other State Parties do not rise because distributional inequalities tend to turn public opinion against globalisation in the form of economic integration and the rules that underpin it.[231] Therefore, we suggest that State Parties retain sufficient regulatory autonomy to address distributional issues within their respective territories. Given that taxes are a significant source of governmental revenue, internal corporate taxes, for example, could be used and structured in a way to address distributional inequalities. However, if cross-border data flows undermine existing

[225] Foster and Azmeh (n 163) 1258. References omitted.
[226] Foster and Azmeh (n 163) 1258. References omitted.
[227] See section 5.1 above.
[228] See Alexander D Beyleveld and Firoz Cachalia, 'Exploring Legal and Policy Options to Address the Competition-Inequality Nexus: The Case of South Africa' in Jan Broulík and Katalin Cseres, *Competition Law and Economic Inequality* (Hart 2022 – forthcoming) in relation to how this might be approached in the South African domestic competition law and policy context.
[229] See, generally, Alexander D Beyleveld, Taking a Common Concern Approach to Economic Inequality: Implications for (Cooperative) Sovereignty over Corporate Taxation (Brill 2022).
[230] See Beth Goldblatt, 'Economic Inequality and the Right to Social Security: Contested Meanings and Potential Roles' in Gillian MacNaughton, Diane F Frey and Catherine Porter (eds), *Human Rights and Economic Inequalities* (Cambridge University Press 2021).
[231] See Alexander D Beyleveld, 'International Cooperation Without Just Distributions? Beginning to Map the Role of Rising Economic Inequality in the Formation and Evolution of and Adherence to International Law' (2021) 14 Law and Development Review 551.

tax revenues, countries might need to introduce alternative types of taxes for new subjects of digital trade. However, in the absence of local presence and data storage, enforcement of such taxation rules might prove difficult. Hence, specified local presence or data localisation requirements could facilitate their enforcement.

5.3.2.2.4 Special and differential treatment for assimilation of lagging State Parties

To accommodate not only the large differences in economic development between African countries but also the different speeds at which they assimilate into the digital and data-driven economies, we recommend designing whatever rules are ultimately deemed necessary on cross-border data flow rules to align markets and support African countries as a whole. This might require the inclusion of special and differential treatment rules for State Parties in need by, for example, allowing less-than-full reciprocity commitments or by extending transition periods for specific obligations whose 'non-compliance' would assist eligible State Parties in 'catching up'.[232] State Parties would need to determine what an eligible State Party is by defining or perhaps listing them. Economic benchmarks could assist in this regard. That said, all AfCFTA State Parties have mandates that likely seek to maximise gains and minimise losses for their own countries, a reality that makes distributive justice difficult to achieve at the continental level.

5.3.2.2.5 Competition rules for disciplining digital MNEs (including platforms)

To address the dominance of Big Techs and any other emerging dominance of digital MNEs (including platforms) within Africa, we suggest reflecting on suitable competition policies that hinder and reduce the development of dominance and anti-competitive behaviour of digital MNEs (including platforms) within the AfCFTA. Anti-competitive behaviour includes when a small number of market-power-wielding firms engage in collusion or exclusionary practices in order to prevent markets from operating as intended to reap disproportionate benefits for themselves. Such practices may consist of, among other things, (i) abusing a dominant position (e.g., controlling data-ownership and distribution, predatory pricing, listing own subjects of digital trade more prominently than those from cheaper competitors), (ii) collectively boycotting competitors, (iii)

[232] See, for example, CPTPP, Article 14.18, and chapter 19, Annex 19-A to the USMCA.

forming cartels, or (iv) concluding other exclusive and anti-competitive agreements such as anti-competitive mergers, market-sharing agreements, inter-firm agreements that involve restrictive arrangements between firms along a distribution line of products, and bid-rigging agreements. This all comes with risks of creating barriers to potential competitors entering a given market.

Notably, the freer the flow of cross-border data, the more competition – whether fair or otherwise – from outside the AfCFTA is permitted. While it is generally true that the more competitors are allowed into a market, the more likely it becomes for that market to trend towards one that is free of players that wield market power, it is also perfectly plausible – and based on experience, likely – that the conduct of digital MNEs (including platforms), if not disciplined in the African market, would be anti-competitive in nature. This could, in turn, prevent markets from operating as intended. Dominant digital MNEs (including platforms) could – and most digital MNEs certainly possess enough power to do so – consolidate their market position. As a result, smaller competitors may be (further) displaced or their market entry impeded. This affects their competitiveness, generally restricts competition, and may adversely affect the diversity of product offerings in the long term. As such, there is a need for regulation and policies that counterbalance these tendencies and prevent, or at least reduce, distortions by disciplining digital MNEs (including platforms) in ways that are geared at markets working as theoretically intended. Indeed, proper functioning markets – i.e., markets that get as close to being perfectly competitive as is possible – tend to be the predominant aim of competition and are broadly considered to be essential to a dynamic and healthy economy. Crucial to achieving the appropriate balance across markets through regulation is usually competition law and policy. Not only do they regulate anti-competitive business practices, but they also strive for a balance between over- and under-enforcement of competition law.[233] They also have the potential to contribute to greater levels of economic equality within jurisdictions.[234]

---

[233] Franziska Sucker and Jonathan Klaaren, 'Trade and Competition (Laws): Interrelations from Southern African Perspective' in Franziska Sucker and Kholofelo Kugler, *International Economic Law: (Southern) African Perspectives and Priorities* (Juta 2021) 565.

[234] See generally Jan Broulík and Katalin Cseres, *Competition Law and Economic Inequality* (Hart 2022 – forthcoming).

It is true that multilateral competition rules alone would go a long way towards ensuring that the cross-border economic activities of digital MNEs (including platforms) are subject to uniform rules irrespective of which country's or region's market is affected. This would, in turn, provide legal certainty for gaps at the regional or national level.[235] We wish to highlight that, in the absence of cross-border competition disciplines that are aimed at constraining the potentially anti-competitive behaviour of digital MNEs (including platforms), it is likely that digital and data-driven product markets will become highly concentrated and large global players will be allowed to (further) entrench their dominant positions in African markets. This would, in turn, lead to the rise of highly distorted markets (if they do not already exist) and further displace small and medium-sized digital MNEs (including platforms) and, thus, deepen pre-existing inequalities.[236] Notably, small- and medium-sized enterprises (SMEs) represent the majority of market players in many African markets,[237] which is why the importance of competition rules cannot be overemphasised.

Of further importance is the idea that, to be effective, competition rules must be developed beyond the traditional confines of the discipline and must be tailored to the particularities of digital and data-intensive industries. In digital and data-intensive industries market power derives from access to large data sets pertaining to large customer bases. In these markets, digital MNEs (including platforms) do not compete in the market, but actually constitute the market itself, an upshot of which is that firms seek to displace each other entirely (as opposed to merely driving

[235] Franziska Sucker, 'The International Trading System and Market Distortions: Revisiting the Need for Competition Rules within the WTO' [2019] *Hungarian Yearbook of International and European* Law 169; Sucker and Klaaren (n 233).
[236] See Sucker and Klaaren (n 233).
[237] See generally Simon Roberts, Thando Vilakazi and Witness Simbanegavi, 'Competition, Regional Integration and Inclusive Growth in Africa: A Research Agenda' in Jonathan Klaaren, Simon Roberts S and Imran Valodia (eds), *Competition Law and Economic Regulation: Addressing Market Power in Southern Africa* (Wits University Press 2017) 263–287. In emerging economies, including in Africa, SMEs contribute significantly higher than 40 percent of GDP (see World Bank, 'Small and Medium Enterprises (SMEs) Finance: Improving SMEs' Access to Finance and Finding Innovative Solutions to Unlock Sources of Capital' <https://www.worldbank.org/en/topic/smefinance> accessed 20 September 2022). See also Celestin Monga and Justin Yifu Lin, 'Introduction: Africa's Evolving Economic Policy Frameworks' in Celestin Monga and Justin Yifu Lin (eds), *The Oxford Handbook of Africa and Economics* (Oxford University Press 2015) 1–20.

other players out of the market).[238] The use of algorithms, which is central to AI technologies, data fusion and app-based transactions, among others, would also need to be accounted for before effective rules can be adopted. This includes answering various pertinent questions, which naturally arise, such as:

- → what the relevant market is;[239]
- → whether and to what extent data can be decolonised;
- → what the relationship between market share and control over data is;
- → what must be included in market shares (e.g., including intangible assets such as reputation and digital control);[240]
- → which public policy goals would contribute to enhance competition;
- → how to address data ownership;
- → how to confront data capitalism as a whole;
- → how to distinguish predatory pricing from innovative-driven price reductions;[241]
- → how to counter network effects;
- → what the effect of data sharing would be;[242] and

[238] Organisation for Economic Co-operation and Development, 'Big Data: Bringing Competition Policy to the Digital Era' (Background Note by OECD Secretariat, DAF/COMP(2016)14, 2016) 17 <https://bit.ly/3dyYuEK> accessed 20 September 2022.

[239] For example, whether Uber provides transport or technology services (see Banga, Macleod and Mendez-Parra (n 143) 21).

[240] Banga, Macleod and Mendez-Parra (n 143) 21.

[241] Banga, Macleod and Mendez-Parra (n 143) 21.

[242] Sharing data at a regional level can be more productive for African countries within the existing regional economic communities, given the potential for economic scalability (see United Nations Conference on Trade and Development, 'South-South Digital Cooperation for Industrialization: A Regional Integration Agenda' (UNCTAD policy brief, 2018) <https://bit.ly/3SgbzS9> accessed 20 September 2022). This will allow for pooling of regional data and digital capacity and the use of digital infrastructure within regions to process regional data. There is significant interest among African private sectors in developing and selling on regional platforms and in intra-regional data sharing (see Banga, Macleod and Mendez-Parra (n 143)).

→ what the cost and benefits of requirements to make data accessible to competitors are.[243]

Since recommendation regimes of digital sales platforms generate a large share of their sales, a possible avenue to consider for reducing risks of abusive behaviour might be prohibiting retail platforms from themselves selling products, services and other trading subjects via the platform, as well as ensuring that purchase records of consumers do not flow into the engine that underpins that platform's recommendation regime.[244] While these are merely options that could be considered, greater cross-border collaboration on competition issues, regardless of what specific approach is ultimately adopted, would likely assist in preventing digital MNEs (especially platforms) from exploiting their ability to control entire markets.

It falls well beyond the scope of this report to elaborate further on cost and benefits of possible competition rules and policies in the digital and data economies context. However, it is worth alluding to the fact that the EU appears to be aiming at making its Digital Services Act a global standard.[245] The manner in which this trend develops should be closely followed by AfCFTA Digital Trade Protocol negotiators because the leading digital MNEs (including platforms), at least from a global perspective, are not based in the EU. Thus, the EU's interest lies in asserting regulatory control over digital platforms within Europe, but also beyond. The aim is to discipline foreign digital MNEs (including platforms), and not merely to shield European digital MNEs (including platforms) from competition 'but to have a healthy competition and to curb data capitalism'.[246] While African countries have similar interests, the EU is a far larger consumer market. As a result, dominant digital MNEs (including platforms) are likely to accept the EU's regulations and, to a large degree, abide

---

[243] See Commonwealth Secretariat, *The State of the Digital Economy in the Commonwealth* (Commonwealth Secretariat 2020); United Nations Economic Commission for Africa, African Union, and United Nations Conference on Trade and Development, *Next Steps for the African Continental Free Trade Area* (United Nations Economic Commission for Africa 2019); Peng (n 195) 213; Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the Digital Era* (European Commission, Directorate-General for Competition 2019) 47 <https://data.europa.eu/doi/10.2763/407537> accessed 20 September 2022; Australian Competition & Consumer Commission, *Digital Platforms Inquiry: Final Report* (Commonwealth of Australia 2019) 57.

[244] See Richard Hill *Development-orientated E-commerce Proposals* (April 2019) paragraph 2.2.8 <http://www.apig.ch/Development%20proposals.pdf.> accessed 20 September 2022.

[245] Peng (n 195) 227.

[246] Peng (n 195) 227.

by them. The same may not be true of regulations sought to be imposed by African countries (although African countries acting as a collective via the AfCFTA are far more likely to succeed at such an endeavour).

5.3.2.2.6 Measures for bridging the digital access divide

To address the low internet penetration and slow broadband speed within African countries, and, thus, the digital access divide, African countries need to develop their digital / broadband infrastructure and make access more affordable.

Attracting inward FDI for digital / broadband infrastructure projects is one possible avenue to counter the digital access divide. However, market access commitments in GATS Mode 3 (foreign investment) in the telecommunication sector has not, thus far, resulted in a more developed, advanced, or affordable broadband infrastructure in developing countries. Neither are such commitments sufficient. Market forces alone without legal safeguards do not increase competition for broadband investment in infrastructure,[247] and may even widen the digital access divide. Broadband operators focus on investing in the most profitable areas of broadband infrastructure development, which is often high-usage, as well as high-volume, low usage business in dense urban areas as opposed to rural areas or low-usage households.[248]

In negotiating the AfCFTA Digital Trade Protocol, State Parties could consider including a specific exception for measures that aim at bridging digital divides, both within Africa, as well as between African countries and non-African countries. Mitigating the digital divide could include, for example, providing tax incentives to broadband operators to serve what would otherwise be non-viable areas from an economic standpoint. A specific exception would prevent 'interpretation stretches' of broad terms such as 'public morals' (as done, for example, in the WTO *Brazil – Taxation* dispute),[249] which were not incorporated with digital divides in mind. To prevent abuse, the

[247] On the need for legal safeguards to ensure competition, see section 5.3.2.2.5.

[248] For greater detail in this regard, see J Gregory Sidak and Daniel F Spulber, 'Deregulation and Managed Competition in Network Industries' (1998) 15 Yale Journal on Regulation 32, 117;120-125; Peng (n 195) 211.

[249] See in this regard WTO Panel Report, *Brazil – Certain Measures Concerning Taxation and Charges* (WT/DS472/R, 11 January 2019), where the panel found that bridging the digital divide even fell within the meaning of 'public morals'

provision may focus on the necessity of the measure to actually bridge the digital divide in a tangible way.[250] However, since this would only serve as a justification for states rather than an obligation, we recommend considering the inclusion of a provision, or set of provisions, that requires cooperation geared at bridging digital divides,[251] namely an obligation to cooperate in good faith to reduce digital disparities of various kinds between and within all AfCFTA State Parties.

Finally, given that broadband infrastructure sources are scarce (e.g., frequencies, telephone numbers, IP addresses, domain names, rights-of-way), State Parties require regulatory space to administer allocations 'in an objective, timely, transparent, and non-discriminatory manner, in the public interest'.[252]

5.3.3 Non-economic rationales and striking a balance

Most non-economic rationales are likely to require some level of restrictions to cross-border data flows. Here African countries have similar regulatory agendas in comparison to most other countries, which include goals such as privacy protection, consumer protection, cybersecurity, law enforcement and national security. More prominent than in other regions might be concerns in relation to job losses and digital access divides. In some jurisdictions, it has already been contemplated whether access to digital / broadband internet should not be accorded the status of fundamental right.[253]

Discussing the benefits and drawbacks of measures potentially employed to achieve these goals is, again, beyond the scope of this report. Though, at this juncture, it is too necessary to collect data to ensure that evidence-based decisions can be made and implemented. Moreover, since the pursuit of certain economic and non-economic goals is often not mutually exclusive, with access to

---

under Article XX(a) of the GATT, but the relevant measure did not pass the necessity test, i.e., the discrimination was not found to be necessary to achieve digital inclusion.

[250] See, for example, CPTPP, Articles 14.13 and 28.12. Similarly, see USMCA, Article 19.11.

[251] See Andrew D Mitchell and Neha Mishra, 'Digital Trade Integration in Preferential Trade Agreements' (Asia-Pacific Research and Training Networks on Trade, Working Paper 191, 2020) <https://bit.ly/3r9GLat> accessed 20 September 2022.

[252] Hill (n 244) paragraph 2.2.2.

[253] For greater detail in this regard, see Peng (n 195) 17 et seq elaborating on examples in Finland, the United Kingdom and Taiwan.

digital infrastructure being a case in point, we suggest that these rationales be considered alongside the economic benefits and drawbacks discussed above.[254] To reiterate, issues related to data control, including who controls it and where it is controlled, must be a key factor in thinking about how to approach the regulation of cross-border data flows, not only because these issues influence the economic benefits that can be reaped from trade, but also from the perspective of regulation designed to protect individual's privacy in relation to their personal data and other non-economic objectives.

Be that as it may, an appropriate balance will still need to be struck between all relevant rationales and policy goals, whether economic or non-economic in nature. It is important to consider some of the consequences – both intended and unintended – certain restrictions might have. These include reducing a platform's openness and stability,[255] impeding access of information,[256] disrupting communication, increasing costs, and reducing data security. These consequences may impede economic and productivity growth, and innovation, both domestically and globally.[257] Some restrictions, such as those which enable censorship, may even undermine human rights (e.g., freedom of expression) or scientific progress,[258] while other filtering measures

[254] See section 4.1.1.

[255] Bildt (n 50); Box (n 50); Hill (n 48) 32; Leslie Daigle, 'On the Nature of the Internet' (Centre for International Governance Innovation and Chatham House Paper Series, Paper No 7, 2015) <https://bit.ly/3SkneQa> accessed 20 September 2022; Clark and others (n 48).

[256] Hill (n 48); Clark and others (n 48).

[257] Keith E Maskus and Jerome H Reichman, 'The Globalization of Private Knowledge Goods and the Privatization of Global Public Goods' 7 Journal of International Economic Law 279; Abdul Waheed Khan, 'Universal Access to Knowledge as a Global Public Good' (Global Policy Forum) <https://bit.ly/3xAt2wE> accessed 20 September 2022; Organisation for Economic Co-operation and Development, 'Economic and Social Benefits of Internet Openness' (OECD Digital Economy Papers, No 257, 2016) <https://bit.ly/3Uhz2V3> accessed 20 September 2022.

[258] Swedish Board of Trade (n 41) 52; Organisation for Economic Co-operation and Development (n 260); Susan Ariel Aaronson, 'The Digital Trade Imbalance and Its Implications for Internet Governance' (Centre for International Governance Innovation and Chatham House Paper Series, Paper No 25, 2016) <https://bit.ly/2CG6NsU> accessed 20 September 2022.

such as 'take down' requirements might be aimed at fulfilling the so-called right to be forgotten (to the extent that it is recognised in a given jurisdiction),[259] or protecting IP rights.[260]

To include a specific provision or section in the AfCFTA Digital Trade Protocol might be more suitable for accommodating the precise balance needed for a particular concern rather than including a general exception for all 'legitimate public policy objectives' with a mere focus on the measure's necessity, as done, for example, in the CPTPP and the USMCA.[261] The latter would also allow for employing trade policy objectives as opposed to only non-trade goals, which general exceptions are usually restricted to in trade agreements.

5.3.4 Taking a holistic approach for the short, medium, and long term

To ensure that trade distortive restrictions to cross-border data flows are not considered in a vacuum but in proper context, i.e., by giving proper consideration to other issues that must be addressed which are not explicitly and/or directly related to cross-border data flows, we suggest contemplating the benefits and drawbacks of restrictions vis-à-vis the free flow of cross-border data holistically in the short, medium, and long term.

For example, many African countries lack efficient and affordable digital infrastructure. While infrastructure challenges are not directly related to the regulation of cross-border data flows, efficient and affordable (broadly inclusive) digital infrastructure is a pre-requisite to meaningful participation in the evolving digital and data economies and for taking advantage of the economic benefits which stem from cross-border data flows. In the short run, this implies the need for a specific set of policies such as identifying, coordinating, and boosting initiatives that work towards an enabling environment for broadband infrastructure development and building relevant capacity. Even though there is no guarantee that China will invest equally where most needed, one such initiative is the Digital Silk Road (DSR) programme. While the DSR programme is certainly

[259] Much of the jurisprudence in this regard stems from the EU, where the right is more correctly referred to as the 'right to erasure', and stems from Article 17 of the GDPR. For a good overview of the right to be forgotten / the right to erasure in the EU context, see generally Globocnik (n 180).
[260] For a discussion on this in the EU context, see Bulayenko and others (n 181).
[261] See, for example, CPTPP, Articles 14.13 and 28.12. Similarly, see, USMCA, Article 19.11.

driven by China's interest to assert itself as the dominant technological power in the world, it may assist in enhancing digital connectivity and improving broadband access in underserved regions and consequently contribute to narrowing infrastructure gaps.[262] In the medium to long run, infrastructure constraints might remain or might have been removed to a large extent for a greater share of the population. Depending on which outcome follows in the medium to long run, it may, in turn, have implications for policy choices in the short run. While it is clearly difficult to predict what the future holds, State Party policy-makers and negotiators will often need to proceed based on a set of well-thought-through working assumptions.

The same is largely true for other areas of policy and outcomes, including the extent to which populations are prepared for the digital and data economies from an educational standpoint, i.e., the extent to which they are technologically literate, and the extent to which data-intensive firms and industries (are allowed or enabled to) develop over time.[263] As alluded to before, thought must also be given to the kind of tax, competition and social security policies that will, among others, be adopted alongside any rules on cross-border data flows as these policy domains will have an impact on the extent to which regulatory interventions aimed at cross-border data flows are, or are not, beneficial on balance.

5.4 On policy coordination

We conclude here with a return to the challenge of policy coordination among different parts of government in each African country. The striking of an appropriate balance between the different policy rationales for allowing or limiting cross-border data flows ideally involves all responsible departments. It likely implicates the departments responsible for international trade, competition, data protection, cybersecurity, law enforcement and IP enforcement, but might affect other departments too, depending on the rationale in question. More so, once a balance is struck, to

[262] Peng (n 195) 223–224.

[263] This would depend, for example, on the extent to which African countries invest in developing data centres, which is seen as one way among many to assist the development of capacity for data collection, storage, and processing within African countries without reliance on foreign service providers, which could in turn lead to making several industries, such as the cloud storage industry, more economically viable.

achieve the overall goals, all implicated departments must take co-ordinated action. This might prove difficult, given that some of the implicated departments are primarily tasked with ensuring the attainment of non-economic goals and some with securing economic goals. Additionally, when contemplating a particular goal, whether economic or otherwise, thought must be given to the extent to which cooperation with policy-makers in other African jurisdictions is required, i.e., beyond potentially concluding rules on cross-border data flows, in order to ensure that particular goals are achieved.

5.5 On required decisions when establishing rules on cross-border data flows

Even if State Parties share a conceptual understanding of terminology, norms and values, and a conceptual and practical understanding of cross-border data flows, negotiations about the content of the AfCFTA Digital Trade Protocol will not be easy. The many decisions that must be made to establish rules on cross-border data flows, which will likely be difficult to agree on might not be the most exhilarating for negotiators. This must include deciding which issues are most relevant from the perspective of AfCFTA State Parties. Once determined, agreement would need to be reached among State Parties on the extent to which and in what manner to address these identified issues of priority should be addressed. Depending on the level of commitment, this could include, among other things, entering into cooperation frameworks, devising common principles and agreeing to anything from harmonised regulations to unified laws.[264] State Parties can also decide between including hard obligations or merely soft, non-enforceable commitments.[265]

Moreover, the scope of the AfCFTA Protocol on Digital Trade would have to be agreed on. Here, two aspects are of particular relevance. First, it must be determined whether the AfCFTA

[264] In a recent survey of African tech SMEs, the most frequently cited priorities for boosting cross-border e-commerce (not digital trade or data flows) were harmonising laws, including in relation to taxation, digital signatures, e-transactions, data standards, privacy and consumer protection and building digital trust. See further Karishma Banga and others, 'E-Commerce in Preferential Trade Agreements: Implications for African Firms and the AfCFTA' (Overseas Development Institute Report for the United Nations Economic Commission for Africa 2021) <https://bit.ly/3QY3wIO> accessed 20 September 2022.

[265] For example, the e-commerce chapter in RCEP is not enforceable via a dispute settlement mechanism. See Jane Kelsey, 'Important Differences between the Final RCEP Electronic Commerce Chapter and the TPPA and Lessons for E-Commerce in the WTO' (bilaterals.org, 10 February 2020) <https://bit.ly/3BwUgFG> accessed 20 September 2022.

Protocol on Digital Trade should apply to all measures that relate to subjects of digital trade or only to those that are currently not covered by the Protocols on Trade in Services, on Trade in Goods, and on IP (once concluded).[266] We suggest contemplating subjecting all such measures to the AfCFTA Protocol on Digital Trade as *lex specialis* and apply the other Protocols as *lex generalis* for purposes of covering gaps and issues of a more general nature. This would account for the fact that (i) State Parties must act consistently with their WTO obligations and commitments, which are similar to those included in the AfCFTA, and (ii) the rules in the Protocols on Trade in Services, Trade in Goods, and IP (once concluded) serve specific and different purposes that might be more accurately addressed within the confines of those protocols. This relates closely to deciding which issues to include in the AfCFTA Protocol on Digital Trade and which issues might be better dealt with as part of the traditional areas of trade negotiations because they can be more effectively dealt with under one of the other Protocols (e.g., goods,[267] services,[268] trade facilitation,[269] IP,[270] competition,[271] or investment).[272] While we anticipate several overlaps, the cross-border data flow and digital trade issues that go beyond the conventional trade issues and seem specific to data flows and digital trade and, thus, specific to the AfCFTA Protocol on Digital Trade ostensibly include (1) data governance rules and regulations,[273] (2) data flows,[274] (3) electronic and digital-

[266] It goes beyond the scope of this report to illustrate the classification problems, which we will address elsewhere in future.

[267] For example, through improving rules of origin, or eliminating tariffs on infrastructure equipment.

[268] For example, defining service sectors that accommodate technological developments, including digitally enabled services. While technological neutrality has been confirmed in WTO jurisprudence in relation to GATS commitments (see, for example, WTO Appellate Body Report, *United States – Measures Affecting Cross-border Supply of Gambling and Betting Services* (WT/DS285, 20 April 2005)), specific stipulations have the potential to prevent legal uncertainty about a sector's scope.

[269] For example, through implementation of rules on e-logistics, paperless trading, single windows, electronic customs processing, digital payments, and *de minimis* thresholds.

[270] For example, through implementation of rules on source codes and algorithms, cybertheft of trade secrets, technology transfer, and clarifying the responsibility for (quality) of products that have been 3D printed based on licences.

[271] See further the discussions under section 5.3.2.2.5 above.

[272] For example, through applying traditional investment rules in relation to things like crowdfunding.

[273] For example, data protection (privacy protection), portability, and security.

[274] For example, data localisation, cybercrime, and third party liability.

transactions,[275] (4) digital taxation,[276] and (5) general principles for measures that relate to subjects of digital trade.[277]

Of course, it almost goes without saying that there will be a plethora of additional decisions which must be made to establish rules on cross-border data flows under the AfCFTA, including on when governments can act inconsistently with their obligations to encourage trade flows or to achieve (other) legitimate policy objectives such as protecting privacy, national security, public morals, or the bridging of digital divides. There remains a long way ahead.

[275] For example, online payments, online contracts, digital certificates, and e-signatures.
[276] For example, duties on electronic transmissions or the implementation of digital services taxes.
[277] For example, application of the most-favoured nation principle, national treatment, cooperation, transparency, implementation, and the relationship between the Protocol and national laws.

ABOUT THE MANDELA INSTITUTE

The Mandela Institute is a centre in the School of Law of the University of the Witwatersrand. The Mandela Institute conducts research, develops policy and offers basic and advanced learning options in different areas of law. The Institute also conducts executive training and capacity-building. For more information on the Mandela Institute, visit www.wits.ac.za/mandelainstitute

ABOUT THE CENTRE FOR THE STUDY OF THE ECONOMIES OF AFRICA

The Centre for the Study of the Economies of Africa (CSEA) is an independent non-profit research organization. It serves as a forum for quality research analyses, and policy dialogue by stakeholders from the private sector, government, national assembly, and civil society. The policy-oriented research carried out by the Centre, including the articulation of policy choices, trade-offs and implications, is put forward to the general public and decision-makers to stimulate rigorous debates on the effects of government policies on economic growth and development in Nigeria and Africa. For more information on CSEA, visit https://cseaafrica.org/

ABOUT THIS REPORT

This report was produced by the Mandela Institute with generous financial and editorial support from the Centre for the Study of the Economies of Africa.

ABOUT THE AUTHORS

Alexander Beyleveld is a Senior Researcher at the Mandela Institute. He holds a PhD in Law from the University of Bern.

Franziska Sucker is an Associate Professor at the Wits School of Law. She holds a PhD in Law from Goethe University Frankfurt.