POLICY BRIEF 01

MANDELA INSTITUTE

DATA PROTECTION IN KENYA, NIGERIA AND SOUTH AFRICA IN THE 2020s AND BEYOND

Introducing a Mandela Institute research project

Alexander Beyleveld

MANDELA INSTITUTE, SCHOOL OF LAW,
UNIVERSITY OF THE WITWATERSRAND

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG

CONTENTS

1. INTRODUCTION

The global economy tends most often to be characterised by what is novel about it at a given point in time. This is especially true during the epochal shifts that are most often styled as 'industrial revolutions'. During the First Industrial Revolution, it was the mechanisation of certain production methods, advances in chemistry, as well as the increasing reliance on steam power – all technological advances, among many others – that were so central to the other trends, such as the increased agricultural productivity, occupational specialisation and demographic growth that were later deemed to characterise that era. Similarly, the Second Industrial Revolution came to be characterised by the technological advances which enabled the widespread adoption of technologies such as the telegraph, railroad networks, sewage systems, gas supply, water supply, electrical power and telephones; while the Third Industrial Revolution has become characterised by further advances in information and communication technologies, most of which relate in some way or another to digitisation and the invention of the Internet, together with the consequent digitalisation these developments brought.

The technological advances that characterise each industrial revolution also had implications for globalisation. Those of the First and Second Industrial Revolutions were responsible for what Richard Baldwin terms 'globalisation's first unbundling'.[1] In essence, what this meant was that international trade boomed due to falling trade costs.[2] It also led to what Kenneth Pomeranz termed 'the Great Divergence', that is, the economic gap between the group Baldwin calls the 'G7' countries (Canada, France, Germany, Italy, Japan, the United Kingdom and the United States) and the rest of the world grew significantly and rapidly.[3] These economic trends also drove the types of economic integration that occurred, that is, the formal and informal legal and policy mechanisms adopted by a set of countries that to varying degrees result in the reduction of barriers to commerce between them. The types of integration were driven to a great extent by the geopolitical power structures generated by the Great Divergence.[4]

During 'globalisation's second unbundling', driven by the technological advances that have come to characterise the Third Industrial Revolution, the Great Divergence became the 'Great Convergence' as communication costs dropped, know-how began to flow across borders and production became increasingly fragmented.[5] The Great Convergence entailed rapid economic growth in a significant number of countries – led by the likes of China, South Korea and India – that far outstripped growth in the G7 countries, thus leading to a rapid reduction in the economic gap between these countries and the G7 countries.[6] As the Great Convergence unfolded, different economic integration trends began to emerge, again driven by shifts in geopolitical power structures.

Broadly speaking, there seems to be consensus that we are currently living through the Fourth Industrial Revolution (or, as the term is commonly abbreviated, '4IR'). As with the three 'revolutions' that preceded it, the 4IR is a complex phenomenon, at the heart of which lies disruptive technological advances and their wide-scale application. These advances have begun, and are likely to continue, to drive the economic trends of our time, as well as the types of globalisation and economic integration we are seeing and are likely to see in the coming years and decades. Against this backdrop, the aim of this policy brief is to introduce a research project which broadly pertains to data – perhaps the key element underpinning the 4IR – and how data are protected in Kenya, Nigeria and South Africa.

The 4IR is a complex phenomenon, at the heart of which lies disruptive technological advances and their wide-scale application.

The second part of the policy brief will discuss the technological and consequent economic and political trends that characterise today's global economy. Within the context sketched in the second part, the third part of the brief will introduce the idea of 'data' and elaborate on a theoretical framework for discussing its economic implications. Equipped with the language developed in the third part, the brief will then introduce the notion of 'data protection' and discuss the apparent trade-off between data protection and cross-border data flows. The ultimate aim is to briefly set out from a transnational perspective what integration options are open to Kenya, Nigeria and South Africa insofar as data protection and cross-border data flows are concerned. With the introductory remarks of parts two through four acting as basic context, part five concludes the brief by setting out what is to come from the remainder of the research project.

2. THE RISE OF THE DATA ECONOMY, 4IR AND THE CONTINUING GREAT CONVERGENCE

The Third Industrial Revolution introduced both broadscale digitisation and digitalisation into the global economy. These trends first gave us the notion of the 'digital economy', which is something conceptually distinct from the 'data economy', which developed later thanks in large part to the rise of the digital economy, on which the data economy relies heavily and into which it feeds back. While all definitions that make up the family of 'economy' concepts rely on information to varying degrees, 'data' as used in 'data economy' does not generally simply refer to mere pieces of information as such. Instead, it refers to pieces of information that are electronically collected in bulk with a view to using them – for example, through analysing them systematically in order to make behavioural predictions – for a particular economic (usually commercial) purpose.

What distinguishes the 4IR from the Third Industrial Revolution is the rapid development of technologies that rely on the data generated as a result of the rise of the data economy. The digital economy can – and did – exist without data. This can be – and was – disruptive. What we may think of today as the 'mere' ability to send an email was something incredibly revolutionary not so long ago: amongst other things, it extended the reach of commercial enterprises by enabling them to vastly expand their activities from a geographical standpoint without losing the ability to manage them from a centralised location. Taken together with other Internet-enabled technologies, email gave rise to production fragmentation and, in turn, contemporary global value chains. These have been incredibly disruptive from the standpoint of the structure of international competition – among workers in different countries and among countries in respect of attracting capital.

The technologies of the Third Industrial Revolution also led to other disruptions that did not rely on data, such as greater levels of automation, especially of routine functions. As the digital economy became highly developed, however, the data economy began its ascent, resulting in the production, collection and storage of truly massive amounts of data. These data, taken together with the advances in computing power necessary to work with them and the fast rate of convergence between different technologies that this drives,[7] are what enables the technologies of the 4IR: artificial intelligence, advanced robotics and 3D printing, the Internet of things (IoT), quantum computing and so forth. The 4IR is and will continue to bring with it a different set of disruptions – possibly positive, possibly negative, likely some combination of both for different people in different places – which will depend a great deal on how we think about data and its protection.

Moreover, as the 4IR got underway, the Great Convergence was continuing unabated: it still is to a large degree. While the COVID-19 pandemic has had deleterious economic impacts in virtually all countries, these have been less severe for countries like China and Viet Nam where economic growth in 2020 remained positive despite the pandemic.[8] The year 2020 was less kind to the United States (US) and the European Union (EU), however, where the gross domestic product (GDP) contracted by 3.5% and 6.1% respectively.[9] Against this backdrop, there is an increasingly acrimonious struggle between the US and China, with both countries vying to be the global hegemon. While it plays a less overt part in it, the EU, which wields significant economic power that should not be underestimated, also forms a part of this struggle, which pertains to a great deal of important issues, such as whether democracy is the most effective form of government. As important, perhaps, is that it also goes to who is at the technological frontier, which necessarily implies a struggle for how data and its protection is conceived of and regulated, especially given the centrality of data to the technologies of the 4IR and the ease with which data are able to cross borders.

As the digital economy became highly developed, however, the data economy began its ascent, resulting in the production, collection and storage of truly massive amounts of data.

Within this environment, the dataa economy has become one characterised by the existence of 'winner-take-all' or 'winner-take-most' markets; that is, markets have become highly concentrated, which has obvious implications for the extent to which they are competitive.[10] This, in turn, has significant implications for economic inequality, both among persons and firms.[11] The resulting situation is one where bargaining power between economic agents is increasingly unequal, with an eversmaller group of actors being able to use ever-growing power and information asymmetries to their advantage. This in turn leads to further market concentration, especially when artificially intelligent

machines are far more capable of extracting value from massive amounts of raw data than human beings are and this small group of powerful actors are firmly in control of the development and exploitation of these technologies. Again, the Great Convergence plays a role here: as competition between powerful nations intensifies at the technological frontier, so does the perceived necessity for nations to grow 'superstar' firms that are capable of competing with superstar firms elsewhere.[12]

Another characteristic of the data economy – which relies heavily on the digital economy – lies in how value is created and assessed, as well as where that value is created and assessed. This leads to the types of jurisdictional challenges that can make it difficult to effectively implement national-level policies, including in relation to things such as taxation, trade, competition and data protection, amongst many others. For example, if data are produced by the citizens of one country, then collected by a firm from another country and stored by a subsidiary of that same firm in a third country before being processed by a different firm in a fourth country who then sells the result of their processing efforts to a firm in the country the data originated from in the first place, how much value was added where? These questions will have very different answers depending on where and by who they are asked.

While the Great Convergence continues, it would be a mistake to think that the disparities between all the countries in the world are rapidly shrinking. While the vast majority of countries in Asia have caught up significantly to the G7 and other rich countries, the same is not on balance true for countries in Africa and Latin America, where average incomes have consistently shrunk vis-à-vis the global average for longer than 60 years.[13] These trends did not unfold equally within Latin America and Africa, either. For example, incomes in Sub-Saharan Africa shrunk much more significantly relative to the global average than incomes in North Africa.[14]

This leads the discussion to another important characteristic of the global data economy: 'digital divides'. These relate in large part to economic divides, both within and between countries and pertain more specifically to the extent to which different groupings of people are able to benefit from the technologies of the Third and Fourth Industrial Revolutions because being able to effectively utilise digital technologies is a pre-requisite for being able to participate in the data economy. Unpacking all the facets of existing (and potential future) digital divides is a daunting task. As one author puts it, '[g]iven the networked context of inequality, an expansion of the definition of digital divides is one that addresses the multi-dimensional aspect of inequality in a digital age'; that is, '[t]he multi-dimensional approach includes the dynamics of socio-economic position, geographic location, ethnicity and language, as well as educational capacities and digital literacy'.[15] Therefore, while it is well beyond the scope of this policy brief to unpack these divides in a comprehensive manner, it is imperative for us to understand them in order to properly understand the context for debates around data protection, particularly in Kenya, Nigeria and South Africa given both their respective economic positions in the world and the economic position of various groups within each country.

3. THE ECONOMICS OF DATA PROTECTION: A PROPOSED THEORETICAL FRAMEWORK

With this understanding of the global economy in mind, the policy brief turns now to sketch a general economic theory of data markets and then attempts to situate the notion of data protection within it.[16]

First, while we have loosely defined what 'data' is above, it is necessary to discuss the economic nature of data and also data markets in greater detail. Data need to be 'produced' by the person or thing the information in question pertains to and then collected and stored. 'Production' as used here should be distinguished from the mere production or existence of information. Instead, data 'production', for current purposes, refers to information that is collected and stored. They have been 'produced' only once they have been collected and stored. This, broadly speaking, is the supply side of data markets. Once produced, data becomes a factor of production, that is, as an input for producing something else downstream through processing. This is where the demand side of data markets comes from. As in traditional markets, the price of data is determined by supply and demand.

Once produced, data becomes a factor of production, that is, as an input for producing something else downstream through processing.

But the economic characteristics of data are still relatively open to conceptual construction and, as such, are malleable. Whereas it is broadly accepted, for example, that oil is a tradeable commodity in the sense that it can be privately owned as well as bought and sold, the same is not currently true for data. Within the data market construction, this malleability is perhaps best illustrated through thinking about the economic

characteristics of data. The first such characteristic is the extent to which data are (non-)rivalrous. In other words, to what extent does consumption of data by one consumer prevent simultaneous consumption by another? The next characteristic is the extent to which data are (non-)excludable. In other words, to what extent can someone be prevented from using data without providing something in return for it?

These characteristics bring into question a number of things, including the issue of ownership. Are data capable of private ownership? If so, can the owner of particular data decide who is entitled to use it and for what purpose in the same way as traditional commodities? If not, what rules govern access to data? These are all complex questions that are answered in large part by conceptually adjusting what data are through modifying the extent to which they are rivalrous and/or excludable. It also goes without saying that different types of data can be conceived of differently: one can, for example, envision a legal system where certain data are capable of ownership and other data not, with guiding criteria such as intended or actual use and nature of the data in question being dispositive of this question. This is essentially how most legal systems work currently.

By studying the extent to which data markets result in market failures, appropriate regulation can be adopted to avoid them.

Another useful question in this regard is whether the operation of data markets leads to any market failures in the ordinary course. One concern regularly raised, amongst others, is the extent to which data markets negatively externalise privacy. In other words, if data markets are allowed to operate without intervention – that is, no regulatory restrictions are imposed in relation to their production or under which circumstances they may be accessed – will the privacy of the persons whose particular data pertain to be violated or impaired without there being an appropriate cost to the data collector, storer or consumer? By studying the extent to which data markets result in market failures, appropriate regulation can be adopted to avoid them. A central question to this, of course, is how one defines a market failure. In the case of privacy, for example, the definition of privacy is important. As is whether one has a right to privacy and, if so, to what extent this right may legitimately be limited by virtue of regulation or even an individual's consent. This is where data protection comes in.

4. APPLYING A TRANSNATIONAL LENS: DATA PROTECTION AND ECONOMIC INTEGRATION FROM THE PERSPECTIVE OF KENYA, NIGERIA AND SOUTH AFRICA

With this theoretical framework in place, the discussion now turns to how it has and could play out in practice with reference in particular to data protection in Kenya, Nigeria and South Africa as countries that participate in the global data economy and the apparent trade-off that exists between data protection and allowing data to flow across borders.

First, it is important to unpack what the term 'data protection' entails. While it may at first blush seem that the word 'data' as used in the phrase 'data protection' is meant in a broad sense, the manner in which the phrase has generally come to be understood suggests a narrower understanding of the word. The 'data' referred to in 'data protection' are usually limited to personal data, with the word 'protection' generally understood as referring to the safeguarding of this type of data. The definition of the phrase 'personal data', however, varies a great deal more depending on who is doing the defining.

Adopted in 2016, the General Data Protection Regulation of the European Union (GDPR) defines 'personal data' as 'any information relating to an identified or identifiable natural person' where,

> *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.*[17]

The Chinese Cybersecurity Law of 2017 (CCL) takes a similar approach in its definition of 'personal information', a term which for the purposes of the CCL,

> *refers to all kinds of information, recorded electronically or through other means, that taken alone or together with other information, is sufficient to identify a natural person's identity, including but not limited to natural persons' full names, birth dates, national identification numbers, personal biometric information, addresses, telephone numbers, and so forth.*[18]

The approach adopted in the United States is quite different. There is no single piece of federal legislation which regulates data protection in general. Instead, data are protected by a patchwork of different federal and other laws, which usually use the term 'personal information' as opposed to 'personal data', most of which employ different definitions. One example of a very detailed definition comes from the California Consumer Privacy Act of 2018 (CCPA). The CCPA defines 'personal information' 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' and includes, but is not limited to, a long list of specific examples of what may constitute 'personal information.*

This even included '[i]nferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, [behaviour], attitudes, intelligence, abilities, and aptitudes'.[19] The CCPA also explicitly excludes certain categories of information from its definition of 'personal information': namely 'publicly available information',[20] as well as 'consumer information that is deidentified or aggregate consumer information'.[21]

The Kenyan Data Protection Act of 2019 (KDPA) adopts the same definition as the GDPR almost verbatim.[22] The Nigerian Data Protection Regulation of 2019 (NDPR) adopts the GDPR definition verbatim, but adds a variety of examples of what constitutes personal information, stating that,

> *[i]t can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information (PII) and others [with PII being defined as] information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context.*[23]

The South African Protection of Personal Information Act of 2013 (POPIA) takes a slightly different approach. Instead of defining 'personal data' it defines 'personal information'. It does so in the following terms:

> *[I]nformation relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to … 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; … information relating to the education or the medical, financial, criminal or employment history of the person; … any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; the biometric information of the person; the personal opinions, views or preferences of the person; correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; the views or opinions of another individual about the person; and the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.*[24]

What these and other definitions tend to make clear is that there is a general consensus around what data protection entails in broad terms: that is, data protection relates (albeit in varying degrees) to the safeguarding of personal data or information, which is most often defined as information that is capable of identifying a person (most often a natural person). Given this definition, the ease with which personal data and/or information flows across borders opens up a number of important questions in relation to the transnational regulation of data flows, especially given that cross-border data flows have become ubiquitous and a significant part of global commerce. This implicates economic integration, particularly insofar as the international trade in data is concerned. If the free flow of data across borders is permitted, there is clearly a possibility that the protection of privacy will be externalised by the operation of international data markets. This suggests a potential trade-off between data protection and the free flow of data across borders. The aim of the remainder of this section is to examine what that trade-off means, particularly for Kenya, Nigeria and South Africa.

4.1 Dominant paradigms

While there is some nuance to this proposition, there are no real rules at the multilateral level that govern data flows across borders and there are definitely no multilateral rules in relation to managing the potential trade-off between the free flow of data and privacy protection.[25] The current state of play in managing this trade-off is accordingly characterised by fragmentation,

with the best way of analysing that state of play currently being through approaches adopted by various countries and regions in pursuit of bilateral or plurilateral regional integration efforts. In this regard, there are currently three dominant approaches to the trade-off, each of which is briefly discussed in turn below.

4.1.1 United States

As one commentator puts it, US practice reflects the country's 'regulatory preference for free crossborder data flows and an economic – as opposed to fundamental rights – approach to the protection of personal information in commercial sphere'.[26] This much is evident from its approach in free trade agreements (FTAs), including the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), the United States-Mexico-Canada Agreement (USMCA) and the US-Japan Digital Trade Agreement, as well as the stance it has taken in multilateral negotiations on e-commerce at the World Trade Organisation (WTO). The US standard includes an obligation not to restrict cross-border data flows (including personal data flows), an exception from this obligation and an article on the protection of 'personal information'.

Article 19.11(1) of the USMCA, for example, provides that, '[n]o Party shall prohibit or restrict 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'. Article 19.11(2) provides the exception in the following terms: '[t]his Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, 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 … and does not impose restrictions on transfers of information greater than are necessary to achieve the objective'.

The USMCA does also include Article 19.8, which speaks to the protection of personal information. Article 19.8(1) provides that '[t]he Parties [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'. To this end, Article 19.8(2) provides that 'each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of digital trade' and that '[i]n the development of this legal framework, 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)'.

Article 19.8(3), moreover, provides that '[t]he Parties [recognise] that pursuant to paragraph 2, key principles include: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability' and that '[t]he Parties also [recognise] the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented'. Article 19.8(4), however, indicates that '[e]ach Party shall [endeavour] to adopt non-discriminatory practices in protecting users of digital trade from personal information protection violations occurring within its jurisdiction'.

> There are no real rules at the multilateral level that govern data flows across borders and there are definitely no multilateral rules in relation to managing the potential trade-off between the free flow of data and privacy protection.

Article 19.8(5) states that '[e]ach Party shall publish information on the personal information protections it provides to users of digital trade, including how … a natural person can pursue a remedy … and … an enterprise can comply with legal requirements'. Finally, Article 19.8(6) notes that '[recognising] that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes', indicates that '[t]he Parties shall [endeavour] to exchange information on the mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them' and intimates that '[t]he Parties [recognise] that the APEC CrossBorder Privacy Rules system is a valid mechanism to facilitate crossborder information transfers while protecting personal information'.

The general starting point, then, is that cross-border flows of personal information shall not be prohibited or restricted. The US position does, at least rhetorically, acknowledge the importance of data protection and does allow for deviations from the general rule in exceptional circumstances. It also provides fairly detailed guidance in relation to what constitutes exceptional circumstances. On balance, however, US-led regimes are very liberal when placed on the broader spectrum of

regimes. This approach makes a fair deal of sense when one recalls that the US does not have a general data protection law grounded in fundamental rights.

4.1.2 European Union

The GDPR is a general data protection law grounded in fundamental rights. The starting point in the EU is accordingly quite different.[27] The proposed texts of its ongoing negotiations with Indonesia in relation to the conclusion of an FTA between the two appear to instructively reflect the EU position. The EU wishes to include an article on the protection of personal data and privacy, the first paragraph of which states 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'.[28] As such, the second paragraph of the proposed article indicates that '[e]ach Party may 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' and that '[n]othing in this agreement shall affect the protection of personal data and privacy afforded by the Parties' respective safeguards'. The EU also proposes a paragraph whereby 'a Party's rules and safeguards for the protection of personal data and privacy, including on cross-border data transfers of personal data' are not subject to regulatory cooperation.

This said, the EU does still attempt to indicate that it views the open flow of data across borders to be important through including a provision that indicates that '[t]he Parties are committed to ensuring cross-border data flows to facilitate trade in the digital economy'. To that end, the EU proposes that:

> *cross-border data flows shall not be restricted between the Parties by … requiring 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 … requiring the localisation of data in the Party's territory for storage or processing … prohibiting storage or processing in the territory of the other Party … making the crossborder 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.*

The proposed text also includes a provision that states that '[t]he Parties shall keep the implementation of this provision under review and assess its functioning within 3 years of the entry into force of this Agreement', that '[a] Party may at any time propose to the other Party to review the list of restrictions listed in the preceding paragraph' and that '[s]uch request shall be accorded sympathetic consideration'.

The EU approach is also far more concerned with ensuring that the GDPR does not come into conflict with trade rules. Its approach is thus far more privacy oriented than the US approach, and far less liberal when placed on the broader spectrum of regimes.

The EU approach is accordingly more restrictive than the US approach. Unlike in the US case, the default is not that prohibitions or restrictions on data flows, including personal data flows, are not permitted. Instead, the EU proposes 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). The EU approach is also far more concerned with ensuring that the GDPR does not come into conflict with trade rules. Its approach is thus far more privacy-oriented than the US approach, and far less liberal when placed on the broader spectrum of regimes. It is still generally permissive (and even encouraging) of cross-border data flows, but it does allow parties to retain far greater regulatory control.

4.1.3 China

The Chinese approach has thus far been quite different. While there have been some limited provisions in Chinese FTAs regarding the protection of personal information, China has thus far not made any commitments in its FTAs in relation to cross-border data flows, opting instead to use its domestic laws to regulate both the protection of personal information and data flows. In terms of the CCL, China has set up an entirely different regime in that it requires data localisation in respect of certain data flowing into China (which data should be localised depends on whether the economic operator in question can be defined as a 'network operator' or a 'critical information infrastructure operator'),[29] which both US and EU FTAs seek to prohibit. Moreover, outflows of data are not permitted by default either (whether the data in question constitute 'personal information' or 'important data' in terms of the CCL does not matter in this regard).[30] Instead, they are subject to an outbound 'security assessment'.[31]

The Chinese approach is accordingly the least liberal of the three dominant paradigms in the sense that it has yet to include or propose the inclusion of obligations that relate to data flows in its FTAs. Yet, there is an emerging consensus that China has stricter data protection laws than in the US and that its approach to data protection is even converging with the far stricter EU approach.[32]

4.2 Integration options for Kenya, Nigeria and South Africa

As has been illustrated thus far, there are three dominant paradigms in relation to managing the apparent trade-off between free data flows and data protection. These approaches tend to show that we are still a long way off from a global consensus as to how to approach the trade-off and that the current state of play is therefore best described as being fragmented. Among the dominant approaches, the US approach is the most liberal insofar as cross-border flows are concerned. The US also offers the lowest level of data protection. The European Union offers perhaps the greatest level of data protection and is cautiously pursuing some level of liberalisation in cross-border flows in its FTAs. Finally, there is China, which is offering stricter levels of data protection, with its approach beginning to converge with that taken in the EU. China's approach to cross-border data flows, however, is the least liberal of the three and is fully regulated by its domestic law.

Against this backdrop, Kenya, Nigeria and South Africa have all purportedly adopted general data protection laws.[33] The aim of this research project, at least in large part, is to examine these laws and contemplate what they mean for the economic integration options available to each country in relation to crossborder data flows. In carrying out these assessments, it is worthwhile to take into account as a starting point that the KDPA, NDPR and POPIA are all fairly akin to the GDPR in the sense that they all take a rights-based approach to data protection. Yet, the development needs of Kenya, Nigeria and South Africa differ. The development needs of Kenya differ from those in Nigeria, which differ from those in South Africa, which also differ from those in Kenya but the development needs of these three countries are far more similar to one another than they are to those of the EU and its member states. As such, while the EU's approach to integration may be worth at least examining, it is quite possible that it will not accord with what is required in Kenya, Nigeria and/or South Africa.

It is also possible, however, for these countries to modify the EU approach in order to meet their own particular needs. They could do so, for example, by altering the items included on the EU's proposed positive list. In other words, instead of simply proposing that measures that relate to localisation and outright prohibitions on storage or processing be included on the list of impermissible restrictions, Kenya, Nigeria and/or South Africa could add to and/or remove from their proposed list various types of measures depending on their liberalisation preferences. They could also propose that a party's rules and safeguards for the protection of personal data and privacy, including on cross-border data transfers of personal data, should be subject to regulatory cooperation (whereas the EU approach suggests these rules and safeguards should not be subject to regulatory cooperation).

It is worthwhile to take into account as a starting point that the KDPA, NDPR and POPIA are all fairly akin to the GDPR in the sense that they all take a rights-based approach to data protection.

As for the US approach, it is worth pointing out that there is no reason that it cannot be implemented in a fashion that treats privacy as a fundamental right. This is especially the case if one adopts a modified version of the US approach whereby one expands the exceptional circumstances in which the general rule against prohibitions or restrictions on data flows does not apply. This would be similar to creating a negative list. In other words, Kenya, Nigeria and/or South Africa could propose making it a general rule in their FTAs that data flows, including personal data flows, should not be prohibited or restricted except in specifically enumerated instances (as opposed to the US approach which merely provides a general exception). The US approach could also be adjusted in other ways, for example, through strengthening its provision on the protection of personal information.

The Chinese approach may be attractive from the perspective of a country that is cautious when it comes to binding itself to international rules. As in the case of the EU and the US approaches, it can also be modified as required, for example, by relaxing or strengthening rules on data localisation, by modifying the category of operators to which different types of obligations apply or by not requiring an outbound security assessment (or possibly by modifying what type of assessment is conducted in relation to outbound data). From the perspective of Kenya, Nigeria and/or South Africa, this would mean proposing not to include any provisions on data flows in FTAs they seek to conclude (they could still, however, propose the inclusion of provisions on data protection, as the Chinese have done in some of their FTAs, for example, their FTAs with Australia and South Korea).

It is, of course, possible for Kenya, Nigeria and South Africa to adopt an approach that is completely unique or which combines different elements from the three dominant approaches sketched out above. Ultimately, however, each country will have to assess the various aspects of the trade-off. In doing so, they will have to ask to what extent the general privacy protection laws they have adopted will be effective in the absence of transnational regulation. Simultaneously, they will have to examine what the potential economic benefits and drawbacks are of allowing data to flow freely in and out of their respective countries and to what extent measures can be taken to maximise gains and minimise losses while maintaining an appropriate level of data protection. Answering these questions will require a combination of empirical work on the economic implications of data protection and cross-border data flows and judgment calls that will ideally be based on a clear and principled strategy that is carefully and agilely monitored over time with a view to making appropriate adjustments where necessary.

5. CONCLUSION: NEXT STEPS FOR THIS RESEARCH PROJECT

The aim of this policy brief has been broadly to sketch the backdrop against which this research project plays out. It has discussed the technological and consequent economic and political trends that characterise today's global economy, introduced the idea of 'data', elaborated a theoretical framework for discussing data in economic terms, introduced the notion of 'data protection', illustrated the apparent trade-off between data protection and cross-border data flows and briefly presented what integration options are available to Kenya, Nigeria and South Africa from a transnational perspective in light of this trade-off.

The stage being set, the remainder of this research project will entail deeper dives into select issues touched on in this policy brief. Next, Jonathan Klaaren's policy brief will examine data protection from the perspective of regional competition policy. Regis Simo will subsequently take a closer look at data protection from the perspective of regional free trade in his policy brief. Thereafter, Alexander Beyleveld's follow-up policy brief will take a closer look at the law and economics of data localisation in Kenya, Nigeria and South Africa before Gabriella Razzano explores the concept of data ownership and the implications for data protection. Country research reports on the data protection regulatory framework in Kenya, South Africa and Nigeria will also be published which will explore the impacts of these national frameworks for the economic development objectives in these three countries. Fola Adeleke will wrap up the project highlighting the outcomes of our publications with concrete policy recommendations on data localisation measures and the need for striking a measured policy balance.

ENDNOTES

1 See generally Richard Baldwin, *The Great Convergence: Information Technology and the New Globalization* (Cambridge, MA: Harvard University Press, 2016), 47-78.
2 See Baldwin, *Great Convergence*, 47-78.
3 See generally Kenneth Pomeranz, *The Great Divergence: China, Europe, and the Making of the Modern World Economy* (Princeton, NJ: Princeton University Press, 2000).
4 On this phenomenon, see further 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,' *Law and Development Review* 14 (forthcoming 2021).
5 See Baldwin, *Great Convergence*, 79-110.
6 See Baldwin, *Great Convergence*, 79-110.
7 For a better understanding on this score, see generally Peter Diamandis and Steven Kotler, *The Future Is Faster Than You Think: How Converging Technologies Are Transforming Business, Industries, and Our Lives* (New York, NY: Simon & Schuster, 2020).
8 See IMF Regional Economic Outlook: Asia and Pacific, database, https://data.imf.org/?sk=ABFF6C02-73A8-475C-89CC-AD515033E662.
9 See IMF Regional Economic Outlook: Western Hemisphere, database, https://data.imf.org/?sk=3E40CD07-7BD1-404F-BFCE-24018D2D85D2 and IMF DATAMAPPER, database, https://www.imf.org/external/datamapper/NGDP_ RPCH@WEO/OEMDC/WEOWORLD/EU.
10 For a cogent discussion of these trends, see John Van Reenen, 'Increasing Differences Between Firms: Market Power and the Macro-Economy' (Discussion Paper 1576, Centre for Economic Performance, London, September 2018).
11 See further Van Reenen, 'Increasing Differences'.
12 Again, see further Van Reenen, 'Increasing Differences'.
13 See World Inequality Lab, *World Inequality Report 2018*, economic research report, https://wir2018.wid.world/files/ download/wir2018-full-report-english.pdf.
14 World Inequality Lab, *World Inequality Report*.
15 Bridgette Wessels, 'The Reproduction and Reconfiguration of Inequality: Differentiation and Class, Status and Power in the Dynamics of Digital Divides,' in *The Digital Divide: The Internet and Social Inequality in International Perspective*, eds. Massimo Ragnedda and Glenn W Muschert (New York, NY: Routledge, 2013) 23.
16 The theoretical economic framework depicted here is largely based on the discussions in Yan Carrière-Swallow and Vikram Haksar, 'The Economics and Implications of Data: An Integrated Perspective' (Discussion Paper 19/16, IMF, Washington, DC, September 2019), but appropriate modifications have been made where necessary. This policy brief does not endorse the approach taken in the IMF policy brief in its entirety without reservations, but the language used therein is useful for discussing issues related to data markets.
17 GDPR, Article 4(1).
18 CCL, Article 76(5).
19 CCPA, section 1798.140(o)(1).
20 CCPA, section 1798.140(o)(2).
21 CCPA, section 1798.140(o)(3).
22 See KDPA, section 2.
23 See NDPR, paragraph 1.3.
24 See POPIA, section 1.
25 For more nuanced discussions, see generally Svetlana Yakovleva and Kristina Irion, 'Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows With External Trade,' *International Data Privacy Law* 10, no. 3 (2020) and Svetlana Yakovleva, 'Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade "Deals"?,' *World Trade Review* 17, no. 3 (2018).
26 See Svetlana Yakovleva, 'Privacy and Data Protection in the EU- and US-Led Post-WTO Free Trade Agreements,' in *Coherence and Divergence in Services Trade Law*, eds. Rhea Tamara Hoffmann and Markus Krajewski (Cham: Springer, 2020), 111.
27 The Court of Justice of the European Union's decisions in the *Schrems* cases are a good illustration of how these differences can play out in practice. See further Joshua P Meltzer, 'The Court of Justice of the European Union in Schrems II: The Impact of GDPR on Data Flows and National Security', *Brookings*, August 5, 2020, https://www .brookings.edu/research/the-court-of-justice-of-the-european-union-in-schrems-ii-the-impact-of-gdpr-on-data-flows-and-national-security/.
28 A copy of the proposed text is available at https://trade.ec.europa.eu/doclib/docs/2018/july/tradoc_157130.pdf. Emphasis added.
29 See Jinhe Liu, 'China's Data Localization,' *Chinese Journal of Communication* 13, no. 1 (2020).
30 See Liu, 'China's Data Localization'.
31 See Liu, 'China's Data Localization'.

32 See, for example, Emmanuel Pernot-Leplay, 'China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?,' *Penn State Journal of Law & International Affairs* 8, no. 1 (2020).

33 While there is no dispute as to the KDPA and POPIA constituting general data protection laws, the status of the NDPR is different. The NDPR is a set of guidelines issued by Nigeria's National Information Technology Development Agency (NITDA) in terms of the 2007 NITDA Act. There remains some debate as to whether NITDA in issuing the NDPR acted within the scope of its mandate as set out in the NITDA Act.

POLICY BRIEF 01

MANDELA INSTITUTE

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 teaching in different areas of law. Further, the Institute conducts executive teaching, training and capacity-building through offering short-course certificate programmes, conferences, and public seminars in areas of law and policy which are domestic in operation but are impacted by global developments.

ABOUT THIS POLICY BRIEF

This Brief is part of a series of publications under the Mandela Institute's 2021 research project on The Economic Impact of Data Localisation in Africa. This project is funded by Facebook.

ABOUT THE AUTHOR

Alex Beyleveld is a senior researcher at the Mandela Institute. He holds a PhD in International Economic Law (magna cum laude) from the World Trade Institute, University of Bern.

Mandela Institute, School of Law
School of Law Building
Braamfontein West Campus
University of the Witwatersrand
Johannesburg 2000
South Africa

www.wits.ac.za/mandelainstitute

Design and layout by COMPRESS.dsl | 400407 | www.compressdsl.com