What to Consider Ahead of the AfCFTA Phase II Negotiations: Focus on Digital Trade Policy Issues in Four Sub-Saharan African Countries

Policy Report

Prepared by
Rutendo Tavengerwei, Valary Mumbo
and Beatriz Kira

United Nations
Economic Commission for Africa

Digital Pathways at Oxford

Blavatnik School of Government
University of Oxford

Beatriz Kira *and* Rutendo Tavengerwei,
Digital Pathways, Blavatnik School of Government, University of Oxford,
and Valary Mumbo, *Master of Public Policy, Blavatnik School of Government, University of Oxford*

Paper 16
January 2022

Digital Pathways at Oxford is a research programme based at the Blavatnik School of Government, University of Oxford. It produces cutting-edge research across the fields of public policy, law, economics, computer science, and political science to support informed decision-making on the governance of digital technologies, with a focus on low- and middle-income countries.

This paper is part of a series of papers on technology policy and regulation, bringing together evidence, ideas and novel research on the strengths and weaknesses of emerging practice in developing nations. The views and positions expressed in this paper are those of the author and do not represent the University of Oxford.

Citation:
Tavengerwei, R., Mumbo, V. and Kira, B. (2022). *What to consider ahead of the AfCTFA Phase II Negotiations: Focus on digital trade policy issues in four Sub-Saharan African countries.* Digital Pathways at Oxford Paper Series; no. 16. Oxford, United Kingdom

https://www.bsg.ox.ac.uk/research/research-programmes/digital-pathways

@DigiPathOxf
Cover image: © Shutterstock

United Nations
Economic Commission for Africa

Digital Pathways at Oxford

BLAVATNIK SCHOOL OF GOVERNMENT

UNIVERSITY OF OXFORD

Acknowledgements

The authors would like to thank the interviewees for the invaluable contributions to this study. For insightful conversations and helpful comments to previous drafts of the report, we are grateful to Emily Jones, Elizabeth Stuart, Danilo Barbosa Garrido Alves, Ify Ogo, David Luke, Jamie McLeod, Vahini Naidu, Vitor Ido, Melissa Omino, Dennis Muhambe, Mohamed Diop, Laura Naliaka, Faizel Ismail, Penny Parenzee, Karishma Banga, Franziska Sucker, Aileen Kwa, Quan Zhao, and Gervais Mendy. For support in funding the research that led to this report, we are grateful to the Omidyar Network. For early input and support with the dissemination of findings, we thank the UN Economic Commission for Africa. For support with the copyediting and typesetting of the report, we thank Kirsten Hunter, Beth Keehn, and Nic Farrell

Table of Contents

Tables

Figures

Abbreviations

AfCFTA	-	African Continental Free Trade Area
ARIPO	-	African Regional Intellectual Property Organization
EAC	-	East African Community
ECOWAS	-	Economic Community of West African States
ECTA	-	Electronic Communications and Transactions Act of South Africa
FTA	-	Free Trade Agreement
ICT	-	Information and Communication Technologies
GDPR	-	General Data Protection Regulation of the European Union
NITDA	-	National Information Technology Development Agency
NDPR	-	Nigeria Data Protection Regulation
OAPI	-	Organization Africaine de la Propriété Intellectuelle (Africa Intellectual Property Organization)
OSS	-	open-source software
SADC	-	Southern African Development Community
TRIPS	-	WTO Agreement on Trade-Related Aspects of Intellectual Property Rights
UNCITRAL	-	United Nations Commission on International Trade Law
UNCTAD	-	United Nations Conference on Trade and Development
USMCA	-	United States-Mexico-Canada Agreement
WTO	-	World Trade Organization

1. Executive summary

Realities such as the COVID-19 pandemic have expedited the move to online operations, highlighting the undeniable fact that the world is continuing to go digital. This emphasises the need for policymakers to regulate in a manner that allows them to harness digital trade benefits while also avoiding associated risk. However, given that digital trade remains unco-ordinated globally, with countries adopting different approaches to policy issues, national regulatory divergence on the matter continues, placing limits on the benefits that countries can obtain from digital trade. Given these disparities, ahead of the African Continental Free Trade Area (AfCFTA) Phase II Negotiations, African countries have been considering the best way to harmonise regulations on issues related to digital trade. To do this effectively, AfCFTA members need to identify where divergencies exist in their domestic regulatory systems. This will allow AfCFTA members to determine where harmonisation is possible, as well as what is needed to achieve such harmonisation.

This report analyses the domestic regulations and policies of four focus countries – South Africa, Nigeria, Kenya and Senegal – comparing their regulatory approaches to five policy issues: i) regulation of online transactions; ii) cross-border data flows, data localisation, and personal data protection; iii) access to source code and technology transfer; iv) intermediary liability; and v) customs duties on electronic transmissions. The study highlights where divergencies exist in adopted approaches, indicating the need for the four countries – and AfCFTA members in general – to carefully consider the implications of the divergences, and determine where it is possible and beneficial to harmonise approaches. This was intended to encourage AfCFTA member states to take ownership of these issues and reflect on the reforms needed.

As seen in Table 1 below, the study shows that the four countries diverge on most of the five policy issues. There are differences in how all four countries **regulate online transactions** – that is, **e-signatures and online consumer protection**. Nigeria was the only country out of the four to recognise all types of e-signatures as legally equivalent. Kenya and Senegal only recognise specific e-signatures, which are either issued or validated by a recognised institution, while South Africa adopts a mixed approach, where it recognises all e-signatures as legally valid, but provides higher evidentiary weight to certain types of e-signatures. Only South Africa and Senegal have specific regulations relating to online consumer protection, while Nigeria and Kenya do not have any clear rules.

With regards to **cross border data flows, data localisation, and personal data protection**, the study shows that all four focus countries have regulations that consist of elements borrowed from the European Union (EU) General Data Protection Regulation (GDPR). In particular, this was regarding the need for the data subject's consent, and also the adequacy requirement.[1] Interestingly, the study also shows that South Africa, Kenya and Nigeria also adopt data localisation measures, although at different levels of strictness. South Africa's data localisation laws are mostly imposed on data that is considered critical – which is then required to be processed within South African borders – while Nigeria requires all data to be processed and stored locally, using local servers. Kenya imposes data localisation measures that are mostly linked to its priority for data privacy. Out of the four focus countries, Senegal is the only country that does not impose any data localisation laws.

Although all four of the focus countries seem to favour the **mandatory disclosure of source code**, the study also shows that the countries remain at different stages in their regulation. Currently, only Nigeria expressly requires multinational enterprises to disclose the source code and algorithms of their software before it is dispatched in Nigeria. This is done for security purposes. In comparison, South Africa only requires the mandatory disclosure of source code where the software will be used by government, while Kenya only promotes the use of open-source software for public services. Senegal is the only country that does not have any specific regulations on source code disclosure, although it expressed an interest in mandatory disclosure of source code for public services.

As shown in Table 1, discrepancies also exist in how the four focus countries regulate i**ntermediary liability**. While South Africa and Senegal both indemnify intermediaries where they are unaware of the nature of the content transmitted or stored on their platforms, Nigeria only penalises intermediaries where they are made aware of the illegal content on their platforms but still fail to take it down. In contrast, Kenya has a stricter approach, criminalising any publication of false data or news, wrongful distribution, and so on.

Although the study shows that all four countries share a position on **customs duties on electronic transmissions**, it is also interesting to note that none of the four countries currently have domestic regulations or policies on the subject.

The report concludes by highlighting that, as the AfCFTA Phase II Negotiations aim to arrive at harmonisation and to improve intra-African trade and international trade, AfCFTA members should reflect on their national policies and domestic regulations to determine where harmonisation is needed, and whether AfCFTA is the right platform for achieving this efficiently.

Table 1: Summary of approaches to the different policy issues

Countries		South Africa	Nigeria	Kenya	Senegal
Policy issues	a. Regulation of online transactions (e-signatures + online consumer protection)	• Does not discriminate against types of e-signatures but provides higher evidentiary weight to certain features of e-signatures • Provides specific regulation on disclosure of information by vendor, spam, etc.	• Recognises all types of e-signatures as legally equivalent • Does not yet have clear laws on online consumer protection	• Only recognises advanced e-signatures issued by a Certification Service Provider as valid • Does not currently have specific legislation on online consumer protection	• Only recognises advanced e-signatures validated by handpicked companies as valid • Provides specific regulation on disclosure of information, payment methods, terms of guarantee, etc.
	b. Cross-border data flows	• Combines elements of the EU GDPR, eg. consent by the data owner; and elements of data localisation, eg. the requirement for processing and storage of all data considered critical within South African borders	• Combines data protection regulations similar to the EU GDPR on consent and adequacy with strict data localisation rules, eg. the requirement for telecommunications companies to host all subscribed and consumer data in Nigeria. Data information firms to host national data in Nigeria as well.	• Enforces data protection laws similar to the EU GDPR, eg. consent by the data owner and requirement for adequacy, combined with elements of data localisation, eg. the requirement for data to be processed through local servers where it is for a public service	• Closely follows the EU's repealed Data Protection Directive 95/46/EC, eg. requirement for consent from data subject, and need for legitimate, explicit and specific reasons for transfer to exist
	c. Access to source code and technology transfer	• Requires the mandatory disclosure of source code for software used by government	• Requires mandatory disclosure of source code and algorithms from multinational enterprises before software is deployed in Nigeria	• Promotes use of open-source software in public administration	• Does not have any specific regulation on source code sharing
	d. Intermediary liability	• Only indemnifies intermediaries from liability where they were unaware of the unlawful nature of the content they transmitted, cached, stored or hosted	• Requires that intermediaries take down content once they are made aware that it is illegal	• Criminalises the publication of false data or news, wrongful distribution of obscene or intimate messages, computer fraud, etc.	• Indemnifies intermediaries where they were unaware of the nature of the content they stored
	e. Customs duties on all electronic transmissions	All four countries do not yet have any legislation on customs duties on electronic transmissions. The position of all four countries at the World Trade Organization is that disallowing customs duties on electronic transmissions would be detrimental to developing countries.			

2. Introduction

With advancements in technology, digital trade[2] is on the rise globally,[3] driven by the increase in access to technology and the internet, as well as countries' intentions to maximise the opportunities and economic returns that digital trade avails. In particular, because business models are continuing to adapt to technological development, this has made it easier for individuals and businesses from different jurisdictions to connect and co-ordinate faster within global value chains, and at lower operation costs compared to traditional trade. As a result, businesses now have a wider reach and are able to sell their products to more markets in the world. While digital trade was already experiencing strong growth prior to the COVID-19 pandemic, the requirement to rely primarily on remote transactions accelerated its advancement.

While the advancement in technology and the rapid move to operating online has been a positive change, it raises several issues. A significant digital divide exists between developed and developing countries. Most developed countries have the capacity to leverage opportunities for early investment in technology, which has allowed them to obtain larger market shares and competitive advantage.[4] This also enabled developed countries to lead in the development of regulatory approaches that allow their economies to benefit from digital trade. This leaves developing countries lagging behind and, at times, coerced into adopting fixed approaches. However, because of how China's digital industrial strategy resulted in the rise of its gross domestic product (GDP) share from 26.1% in 2014 to 34.8% in 2018,[5] other developing countries have been encouraged to develop similar regulatory approaches to allow them to catch up with industrialisation, and compete in the global market.

Given the risks that accompany digital trade, countries around the world have begun tackling a wide spectrum of cross-cutting issues, and providing regulation to leverage the economic benefits. Such issues include rules relating to paperless trade, digital taxation, regulatory practices that promote digital competitiveness, online consumer protection, cross-border data transfers, intermediary liability, disclosure of source code, customs duties on e-transmission etc. While efforts exist at the World Trade Organization (WTO) under the Joint Statement Initiative (JSI) and other fora such as the Organisation for Economic Co-operation and Development (OECD), to create a multilateral approach to the regulation of some of these issues, the lack of consensus on how to regulate has created an impasse on global rule-making. As a result, to shape norms related to digital trade in a manner that has an international dimension and that also reduces the chance of trade conflict, countries have been proactively negotiating and agreeing on rules in bilateral and plurilateral trade agreements such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Digital Economy Partnership Agreement (DEPA), United States-Mexico-Canada Agreement (USMCA) etc. This is ensuring that countries uphold the two key aspects of international trade: the most favoured nation principle; and the national treatment principle. In addition to regulating trade agreements, a significant number of countries, such as the UK, US, China, and Australia, have also been at the forefront of developing their own domestic regulatory approaches – with some of these approaches then appearing in related trade agreements. This has resulted in a fragmented ecosystem of rules.

African countries have however not been very involved in the digital trade rule-making process at the multilateral, plurilateral or bilateral level. In particular, at the time of writing of this report, only four African countries were actively participating in talks at the WTO's JSI,[6] while only 25 were part of the OECD's Inclusive Framework.[7] Furthermore, apart from regional initiatives, African countries have not been very active in bilateral or plurilateral trade agreements that focus on trade. As a result, African countries are beginning to endure pressure to negotiate bilaterally – for example, the US-Kenya Trade Agreement negotiations.

Considering the potential gains from digital trade, and the progress that other countries – especially developed countries – have made in regulating the related issues in a beneficial way, there is a need for the African region to carefully consider how best to develop and implement harmonised regulations that are tailored to the region. In particular, the African Continental Free Trade Area (AfCFTA) – which was signed by 54 of the 55 African Union member states, and (at the time of writing), ratified by 41[8] – has the potential to be the platform to achieve this for the region. Therefore, ahead of AfCFTA's Phase II protocol negotiations, it is important that its members fully consider any digital trade related issues in the context of their national and regional, social and economic priorities – taking into consideration the implications of the different international approaches – before definitively adopting or disregarding them. This will also allow AfCFTA members to identify opportunities to create bespoke rules that encourage intra-regional trade for the continent, as well as trade with the rest of the world. This is important because provisions negotiated in trade agreements – be it at bilateral, regional, or plurilateral level – can either constrain or support national or other regional (or eventually, global) policymaking and regulatory efforts aimed at harnessing the benefits of digitalisation.

In terms of general methodology, this report provides a comparative analysis of the different regulatory and policy approaches adopted by four focus countries – South Africa, Kenya, Nigeria, and Senegal – on five specific policy issues. These countries were chosen because they are major economies in the region that are generally active in trade talks, have burgeoning technology sectors, and are proactively involved in the regulation of digital trade. The key policy issues analysed were chosen based on the emerging trends of key issues being negotiated or appearing as provisions in trade agreements globally,[9] which could therefore also be included as part of the AfCFTA's Phase II Negotiations. According to a study by Burri and Polanco, these issues include: the regulation of online transactions; cross-border data flows; access to source code and technology transfer; intermediary liability; and customs duties on electronic transmissions.[10]

By systematically comparing the regulatory approaches of the four focus countries, this report identifies where divergencies in regulation exist, allowing policymakers – those from the four countries as well as other AfCFTA members with similar contexts and economic interests – an insight into the diverse approaches being adopted. With such insight, where the AfCFTA is seeking harmonisation on these issues, policymakers can therefore decide whether they want to harmonise approaches, and if so, which are the most effective.

3. Policy issues in detail

This part of the report discusses each of the five key policy issues. Under each issue, the report details how the policy issue is being regulated internationally, highlighting potential conflicts of these regulatory approaches for the African region if adopted under the AfCFTA. For each policy issue, the report proceeds to a comparative analysis of the regulatory approaches adopted by each of the four focus countries, highlighting where divergences exist.

3.1 Regulation of online transactions

The increase in world-wide online shopping makes digital solutions more relevant – for example, e-signatures that facilitate online transactions – and intensifies the need for online consumer protection. As a result, it has become increasingly necessary for countries to ensure that they regulate online transactions in a way that promotes trust – from consumers as well as service providers.

3.1.1 E-signatures

E-signatures have been a significant feature of digital trade, facilitating the remote conclusion of business contracts between consumers and service providers.[11] E-signatures have also been instrumental in enabling cross-border business-to-business transactions where a contract with specific terms and conditions is necessary to maintain a business relationship over time. However, in spite of the role of e-signatures in cross-border trade, countries are at different stages in their regulations, and hold different positions in relation to technological neutrality – as well as the legitimacy and treatment of e-signatures.[12] This means that, while e-signatures are accepted in several countries, the form of e-signatures recognised as legally valid and equal to handwritten signatures remains the issue of contention.

At the international level, there is yet to be a binding multilateral instrument setting out regulations for e-signatures. Although several countries have been using the United Nations (UN) Electronic Communications Convention as a reference in drafting legislation that promotes technological neutrality and functional equivalence between electronic and hand signatures,[13] governments have mainly been split between three main approaches, which all differ in their legal treatment of e-signatures.

Figure 1: Approaches to regulation of e-signatures

Minimalist approach	Prescriptive approach	Hybrid approach
Countries accept all forms of electonic or digital signatures, eg. US and Australia	Countries require that parties to a transaction must use a specific government-authorised method or technology for signature to be valid, eg. Indonesia	Countries accept all forms of electronic or digital signatures but give higher evidentiary weight to specific types, eg. South Africa

As shown in Figure 1, the regulatory approaches to e-signatures are: minimalist, prescriptive and hybrid.[14] The minimalist approach is mostly adopted by countries with a traditional common law system, such as the US and Australia. Under this approach, countries promote technological neutrality, accepting all forms of electronic or digital signatures,[15] and leaving the decision of the form of signature to the parties of the transaction.[16] This is seen to offer users more flexibility and adaptability and is therefore more consumer-friendly.[17] In addition, the flexibility of the minimalist approach is considered favourable because it allows the market to shape the direction of e-signatures and not stifle innovation by over-regulating them.[18]

However, with the level of uncertainty that exists online, the prescriptive approach is viewed as a means to providing reliability and security, in turn ensuring trust for online users.[19] Countries that have adopted the prescriptive approach – mainly civil law jurisdictions – require the parties to a transaction to employ a specific government-authorised method or technology.[20] For example, for a digital signature to be recognised in Indonesia, it must have been created through a digital certificate provider registered with the Ministry of Communication and Technology using servers located in the country.[21] This approach has the advantage of providing maximum certainty to users.

In contrast, (as its name suggests), the hybrid approach combines features of both the minimalist and the prescriptive approach. Countries that adopt the hybrid approach, such as South Africa, Brazil, China and the EU, provide legal status to all methods of e-signatures, though they accord greater evidentiary weight to methods with certain specific features, for example, digital signatures.[22] The hybrid approach provides the flexibility offered by the minimalist approach, thus achieving technological neutrality, while simultaneously allowing for the legal certainty obtained by the prescriptive approach.[23]

Regional approaches to e-signatures

According to the United Nations Conference on Trade and Development (UNCTAD) Global Cyberlaw Tracker, only 33 countries in the African region have e-transaction legislation; six have draft versions and another six lack any form of legislation[24]. As discussed below, the domestic laws of the recorded 33 countries include a mix of the three approaches shown in Figure 1. In particular, among the four countries in this study, a divergence exists, ranging from purely minimalist to hybrid.

This indicates the countries' range of different interests, and illustrates the complexity involved in reaching any potential harmonisation of laws that countries might want to undertake under the AfCFTA. Having varying regional domestic rules on e-signatures and authentication also makes compliance difficult for businesses that want to operate in multiple countries. This complicates cross-border digital activities and increases the cost of operating in multiple markets. In addition, where consumers from other AfCFTA jurisdictions may have to conduct online transactions, this lack of clarity over relevant legal norms may lower their confidence in e-commerce.[25] Therefore, ahead of the AfCFTA's Phase II Negotiations, it is necessary for countries to take into account the divergencies highlighted below, as well as the associated costs. This will enable AfCFTA members to consider whether, and how, harmonisation or regional regulatory co-ordination can be achieved. These considerations are important for policymakers to create tailored, practical and achievable solutions to ensure that unnecessary costs are not imposed on businesses, especially micro-, small and medium-sized enterprises (MSMEs).

South Africa

South Africa has consistently adopted a hybrid approach to e-signatures. This is employed under the Electronic Communications and Transactions Act off 2002 (ECTA)[26] which is consistent with the principle of technology neutrality in the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Signatures. While South Africa, through its hybrid approach does not discriminate against types of e-signatures, recognising them as legally equivalent,[27] it also provides higher evidentiary weight to certain features of e-signatures. In particular, all vendors' e-signature products must be accredited by the Director General of the Department of Communications.[28]

Nigeria

Nigeria, in contrast to South Africa, Kenya and Senegal adopts the minimalist approach in regulating e-signatures. In line with its commitments under the Economic Community of West African States (ECOWAS) Electronic Transactions Act of 2015, Nigeria generally regards e-signatures as reliable and binding unless there is evidence to prove otherwise.[29] According to Nigeria's Evidence Act of 2011, an e-signature may be proved in any way. This can include procedures prior to a transaction that require an individual to execute a symbol or security procedures to verify their electronic record identity.[30] Therefore the burden of proof regarding the genuineness of an e-signature lies with the individual contending its validity. The country's minimalist stance is in line with regional model law as laid out by the ECOWAS Supplementary Act on Electronic Transactions of 2010.

Kenya

Kenya's approach to the regulation of e-signatures is prescriptive, recognising advanced e-signatures only as valid in electronic business contracts.[31] The use of advanced e-signatures for business in Kenya was introduced by the Business Laws (Amendment) Act of 2020 which amended business-related statutes - including the Law of Contract Act, which now provides for use of advanced e-signatures that would be enforceable during litigation.[32] Advanced e-signatures are considered valid only if issued by a Certified Service Provider licensed by the Communications

Authority of Kenya, and only for commercial contracts.[33] In addition, where a document contains a foreign advanced e-signature, providers of e-signatures, such as DocuSign, can be recognised locally on the condition that they are licensed by their home authorities and adhere to Kenyan law and international standards.[34]

Senegal

Much like Kenya, Senegal also adopts a prescriptive approach to e-signatures. In particular, in line with the UNCITRAL Model Law on Electronic Commerce of 1996, Senegal's domestic law allows for the use of e-signatures as a means of authentication, adopting technological neutrality and equating electronically signed documents to physically signed ones.[35] To guard against fraudulent activity and maintain user trust, Senegal only legally allows handpicked companies[36] to validate signatures, further complicating the authentication process.[37] As illustrated above, Senegal's domestic laws on e-signatures diverge from those of Nigeria and South Africa.

3.1.2 Online consumer protection

Consumer protection for online transactions is another significant area relevant to the regulation of electronic transactions. For consumers to properly conduct and engage in online transactions, the socio-economic aspects of business online must be addressed.[38] There is need to ensure that consumers are guarded against online threats such as virus attacks, spam, card fraud, defective goods, misrepresentation etc.[39] At present, online consumer protection is being regulated based on different approaches. Some governments have relied on the industry to self-regulate, developing methods to ensure security for the consumer when transacting online.[40] Other governments have provided explicit regulation including provisions that address returns, consumer safety, supplier liability and inadequate redress mechanisms in cases where consumers' rights are breached.[41] In trade agreements particularly, several regional agreements such as the Colombia-Northern Triangle and the Canada-Honduras Free Trade Agreement (FTA) contain provisions with 'soft language' where countries recognise the importance of transparent and effective measures and, in turn, endeavour to co-operate on exchanging information on their regulatory approaches.[42] Other trade agreements such as the Association of Southeast Asian Nations (ASEAN)-Australia-New Zealand FTA have stronger language where countries commit to providing the same level of consumer protection, online and offline.[43]

Regional approaches to online consumer protection

Regionally, the Southern African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce has guidelines that set out obligations of an online supplier to provide customers with, for example, full information of the good or service as well as the payment system and terms of agreement, in addition to granting the consumer the right to cancel.[44] In the region as a whole, 25 of the 54 countries have some form of legislation in relation to

online consumer protection, while four have draft legislation, according to UNCTAD. As illustrated below, this study shows that only South Africa and Senegal have specific regulation on online consumer protection, while Nigeria and Kenya do not currently have any legislation. This indicates that the development of regulation of online consumer protection is still in its infancy. However, according to a study with African firms, online consumer protection was identified as a significant barrier to e-commerce. In addition, concerns were raised about improving consumers' trust and providing alternative dispute resolution services, both within countries and across borders.[45] Therefore, in the context of AfCFTA Phase II Negotiations, and because most countries are still in the process of developing their regulatory approaches on this issue, it is important for countries to consider whether it would best serve their interests to agree on strong online consumer protection commitments in a trade agreement. In determining the best way forward, AfCFTA members should also examine whether they have the individual capacities and resources needed to implement and enforce any agreed online consumer protection commitments.

South Africa

South Africa provides explicit regulation of online consumer protection in its domestic laws, aiming to provide legal certainty for online transactions. In addition to obligating online suppliers who sell or hire goods and services online to disclose all relevant information about themselves to the consumer, South Africa's ECTA follows the SADC Model Law on Electronic Transactions and Electronic Commerce and also establishes the terms of the offer and acceptance of an electronic contract.[46] ECTA also establishes that it is a criminal offence to send unsolicited commercial communications (spam) to consumers without providing them with the option to unsubscribe.[47] Criminal charges and penalties may also be imposed if spam messages continue to be sent to a consumer who has already sent a notification communicating that they wish to opt out of receiving the emails. Where a consumer requests how their information was obtained, senders are also obligated to provide such details.[48]

Nigeria

Due to the unfinished state of the law around online consumer protection in Nigeria, the country's position on online consumer protection is presently unclear. While Nigeria's Federal Competition and Consumer Protection Act of 2019 (the FCCP Act) protects several consumer's rights – including to have information presented in plain and understandable language, to be able to examine goods, the right to return purchases etc. – it does not explicitly refer to online products and services.[49] This means that the FCCP Act is ambiguous about the context for online transactions. However, in 2018, the Consumer Protection Council developed principles aimed at addressing issues of online transactions and e-commerce, although there have been no updates on the implementation of the principles.[50] These principles include recognising the importance of providing complete disclosures of any and all transactional terms.[51]

Kenya

While Kenya does not currently have specific domestic legislation relating to online consumer protection, the Kenyan Consumer Protection Act of 2012 (the KCP Act) which guarantees the protection of consumer rights, makes reference to instances where a consumer is protected in an

'internet agreement'.[52] According to the KCP Act's interpretation section, an internet agreement refers to 'a consumer agreement which is formed by text-based internet communications',[53] which can therefore be interpreted to include online transactions. Under the KCP Act, before an online agreement is concluded, the consumer must be made aware of all related terms and conditions, including the circumstances when they can opt to cancel the agreement.[54] However, because the KCP Act does not directly regulate online transactions, it is still silent on other important issues such as spam, misuse of data, and return of goods or services. It remains unclear whether the lack of adequate legislation for online consumer protection is an indication that Kenya is still in the process of working on specific legislation related to online consumer protection, or that it is moving toward industry self-regulation. If it is the former, Kenya must consider how its AfCFTA counterparts have been regulating online consumer protection, and whether similar protections would assimilate well into the Kenyan legal system, providing the intended trust to the online consumer, both in Kenya, and across the region.

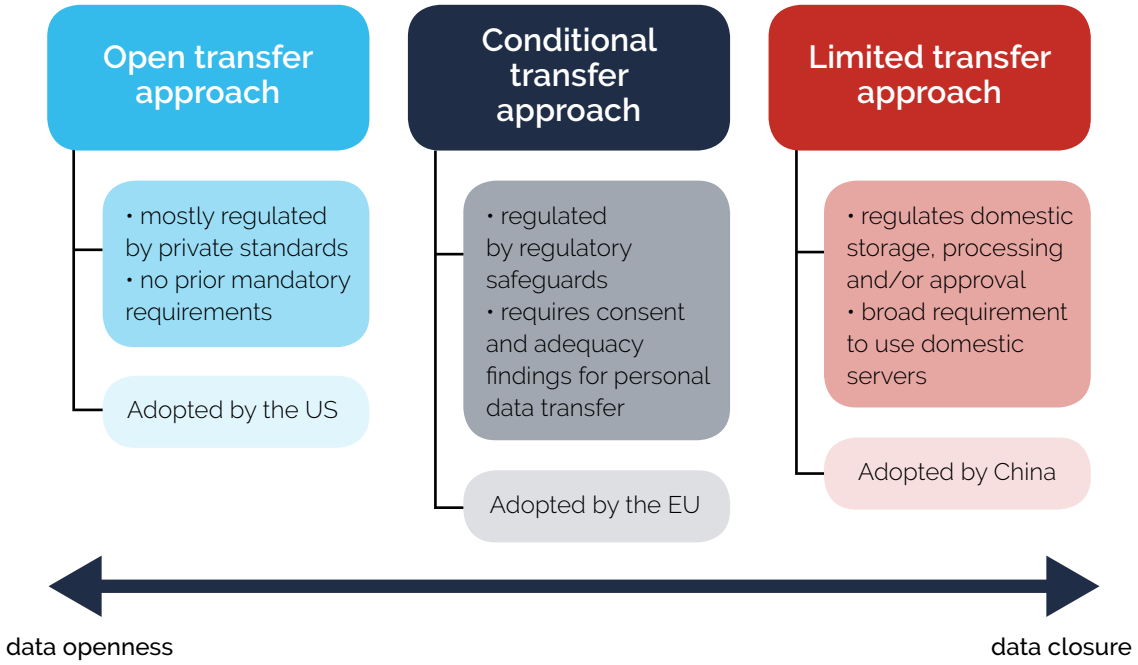
Senegal

By providing explicit regulations on online consumer protection, Senegal aims to balance online consumer rights and online vendor obligations, enforcing rules that ensure that e-commerce platforms are safe and accountable. For example, Senegal's 2008 Decree on Electronic Commerce imposes obligations such as the duty of information, which places responsibility on the online vendor to disclose all relevant information about themselves – for example, their particulars, relevant information about the good or service, methods of payment, terms of the guarantee etc.[55] The Decree on Electronic Commerce provides for rights such as the right of retraction which allows a consumer – in the case where they have concluded a contract with an online vendor – the time frame they have to retract from the contract without facing any penalties.[56] The law also ensures that online vendors are not taken advantage of, by only allowing the right of retraction to be exercised where the online contract of sale provides for a period to try/test the goods or service.[57] Therefore, the onus is placed on the consumer to ensure that, if they decide to retract, they return the goods undamaged. Senegal's Law on Cybercrime also provides for penalties that are applicable if the above regulations are breached.

3.2 Cross-border data flows, data localisation, and personal data protection

Cross-border data flows involve the transfer of digital information – public or private – from one jurisdiction to another. Given the current digital transformation, this is important because both production and trade have increasingly been reliant on storing, moving and using this digital information – with the COVID-19 pandemic accelerating this.[58] To balance the potential economic gains of data flows with domestic policy objectives, countries have been trying to determine the best way to regulate cross-border data flows, including in trade agreements.[59] A few approaches to the regulation of cross-border data flows have been emerging, as shown in Figure 2 below.[60]

Figure 2: Approaches to data transfer[61]



The first approach is 'open transfer', mainly employed by the US.[62] This approach allows for standard-setting and self-regulation by the private sector, prohibiting most restrictions on cross-border data transfer and creating an environment that promotes free flow of data above any protection or privacy offered to the consumer.[63] While encouraging innovation, this approach has been criticised for failing to properly protect consumers' data and disregarding their privacy.

In contrast, the 'conditional transfer' approach – also referred to as the 'privacy-as-priority' approach – used by the EU prioritises individual privacy, with personal data only being authorised for transfer where third party countries have obtained an adequacy determination ensuring that the same levels of data protection are granted.[64] While this approach addresses the issue of privacy, critics argue that it violates the most-favoured nation principle through its adequacy decisions, which subjectively grant special treatment to some countries and not others. It also creates an onerous regime for developing and least developed countries to try and align with.[65]

The 'limited transfer' approach – also widely referred to as the 'data localisation' approach – is employed at varying degrees, mostly by developing countries, including several countries in Africa such as Nigeria and Kenya where the regulatory framework consists of elements of this approach.[66] Data localisation measures usually place requirements for the collection, processing and storage of data before it can be transferred and used across the border.[67] In their variation, data localisation measures range from most restrictive – those that require several conditions to be met before any data can be transferred (e.g, the requirement for data to be processed and stored locally) – to the least restrictive measures – those that only restrict data movement to the extent that the local company decides where to store and process the data.[68]

Data localisation laws can be useful for meeting various policy goals, including: safeguarding fundamental rights such as the right to privacy; promoting inclusive growth and innovation domestically,[69] meeting regulatory needs that necessitate ensuring access to data for supervisory purposes, and; national security on the premise that data localisation decreases the risks of unauthorised access, and so on.[70] In addition, as Foster and Azmeh point out, localisation measures can be used as a modern industrialisation strategy, facilitating the joining of developing economies in complex production networks, and creating opportunities for developing countries to catch up.[71] The Institute of International Finance (IFI) argues that, while it is worthwhile for countries to pursue the above-mentioned objectives, they are mistaken to attribute the realisation of these objectives to data localisation measures.[72] This is because doing so indicates a fundamental misconception about how, and when data gains value. The IFI argues that data localisation measures undermine trade and economic growth by restricting the free flow of data, in turn slowing the digital ecosystem.[73]

Regional approaches to cross-border data flows

Regionally, the African Union's Convention on Cyber Security and Personal Data Protection (the Malabo Convention) holds the most potential as the tool to harmonise regulations on areas such as cross-border data flows and personal data protection and privacy, by all member states.[74] Borrowing legal elements from the EU's Data Protection Directive (which was superseded by the GDPR), the Malabo Convention follows the conditional transfer approach mentioned above, with transfer of personal data being permissible following an adequacy determination, and consent of the data subject.[75] However at the time of writing of this report, only eight countries had ratified the convention – with Senegal being the only country that ratified it, among the four countries analysed in this paper.[76]

Other efforts for a harmonised regulatory system for cross-border data flows have been emerging in the Regional Economic Communities. For example, in 2008 the East African Community (EAC) initiated the EAC Framework for Cyberlaws Phases I and II (the EAC Framework), addressing multiple cyber law issues, including data protection. However, the EAC Framework does not provide specific guidance on the regulatory approach to be adopted by its members; instead, it provides that its members must comply with 'principles of good practice' in relation to all aspects of cross-border data flow.[77] In contrast, the ECOWAS Supplementary Act on Personal Data Protection 2010 (ECOWAS Supplementary Act), specifies the content required of data privacy laws and obligates each member to set up a Data Protection Authority. The ECOWAS Supplementary Act is legally binding, but is only effective when member states establish data protection frameworks. In April 2021, although 11 ECOWAS member states had data protection laws, only four had enacted data protection legislation after the conclusion of the ECOWAS Supplementary Act – excluding Nigeria.[78] In 2013, the SADC also published soft law in the form of a Model Law on Data Protection, which provides guidelines on the enactment of privacy laws,[79] but is not binding on SADC members.

It is interesting to note that all three regional regulatory instruments mentioned above contain elements similar to the EU GDPR in relation to privacy. However, in comparison - as explored below - domestic regulatory approaches to cross-border data flows adopted by the focus countries of this report seem to diverge with the approaches adopted by their respective Regional Economic Communities. For example, in the case of Nigeria, there is tension between the country's data localisation measures and its regional commitments under the ECOWAS Supplementary Act which follows the conditional transfer approach. This divergence illustrates that the regulation and implementation of cross-border data flows at Regional Economic Community level has been challenging. This could be because member countries have varying socio-cultural values and legal cultures.[80]

Therefore, with the AfCFTA digital trade protocol, countries have an opportunity to create legislation that will provide the delicate balance between their national priorities and interests, and economically beneficial laws.[81] This is especially important for the African continent because enormous amounts of data are generated in the region, creating opportunities for countries to harvest significant economic gains from data-driven trade.[82] Minimal variations in rules on cross-border data flows in the AfCFTA are important because they will enable businesses – especially MSMEs, which constitute most of the businesses on the continent – to meet their legal obligations without having to adhere to high compliance costs. However, it is still important that countries consider the implications of each regulatory approach, as well as whether they are equipped with adequate resources for implementation.[83] In addition to determining which approach best serves their interests, this will also allow AfCFTA members to consider whether a single regulatory approach would achieve the social and economic interests of all AfCFTA members, given the cultural and economic differences that exist among them. It will also allow AfCFTA members to determine how harmonisation – or interoperability – if opted for, can be achieved. These are all important considerations given that developing and developed countries are currently polarised regarding the right approach to the regulation of cross-border data flows; and pressure for African countries to subscribe to certain approaches might surface in the negotiation of the AfCFTA's digital trade protocol.

South Africa

In its approach to cross-border data flows, South Africa marries elements of the EU GDPR with some less restrictive data localisation rules. Under the Protection of Personal Information Act of 2013 (POPI Act)[84] –the country's primary legislative instrument on data protection and transfer – South Africa adopted the conditional transfer approach. This means that, for South Africa, personal data is only transferrable to a third country where:

> **(i)** the recipient is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection – one that effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for lawful processing in the POPI Act;
>
> **(ii)** the data subject consents to the transfer;

(iii) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;

(iv) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or

(v) the transfer is for the benefit of the data subject, and it is not reasonably practicable to obtain the consent of the data subject to the transfer and, if it were, the data subject would be likely to give it.

It is clear that, similar to the GDPR, the SADC Model Law on Data Protection and the Malabo Convention, the POPI Act apportions rights to the data subject and obligates data controllers to ensure that, when personal data is being transferred across borders, the recipient country provides an adequate level of protection to that data. In addition, as illustrated below, these elements of the POPI Act are also adopted by Kenya and Senegal.

However, while the POPI Act largely follows the EU GDPR,[85] South Africa's draft National Data and Cloud Policy (published for public comments in April 2021) proposes more data localisation policies to be imposed on cross-border data flows.[86] These include requirements such as the processing and storage of all data identified or classified as critical information to be done within South African borders, as well as requirements for data generated within South African borders – even by a foreign company – to be treated as South African property.[87] Critics of the draft policy have argued that, while it is an attempt for to the government to gain control of locally sourced data, the draft policy's current proposed hard data localisation measures – which somewhat deviate from the regulatory regime created by the POPI Act – have the potential to undermine the protection of privacy and also stifle competition in the cloud sphere.[88] In addition, if these data localisation measures are adopted by South Africa, they would be contrary to the SADC Model Law and the Malabo Convention – though it is important to note that the SADC Model Law is not binding on South Africa, and the country has not yet signed or ratified the Malabo Convention.

Therefore, taking into consideration South Africa's regulations on cross-border data flows overall, it can be argued that South Africa is in the process of developing a type of hybrid approach where it prioritises the privacy of its data subjects, but also seems to have an interest in promoting data sovereignty.

Nigeria

Similar to South Africa, Nigeria also employs a hybrid approach to the regulation of cross-border data flows, although it combines elements of data privacy similar to the GDPR through a conditional transfer approach, with relatively stricter data localisation rules.

Nigeria's Data Protection Regulation of 2019 (NDPR) – which is also currently the governing regulation – requires any transfer of personal data made to foreign countries to be done with approval of the National Information Technology Development Agency (NITDA) and the Attorney General's supervision.[89] This is to ensure that the legislative adequacy of the destination country

offers the same level of protection as Nigeria. However, a few exceptions exist for data to be transferred without approval. These include: where data subjects have expressly consented to the transfer; where it is necessary for the performance or the conclusion of a contract between the data subject and another party; or where the transfer is in the public interest.[90] The law also outlines penalties that can be imposed on data controllers for violation of these regulations – this is based on the number of legal data subjects they are dealing with.[91] NITDA is in charge of the implementation of the provisions of the NDPR and is responsible for the registration and licensing of Data Protection Compliance Organisations to monitor, audit, conduct training and data protection compliance consulting on its behalf. In addition, the NDPR guarantees a high level of data privacy to Nigerian companies and citizens.[92] Interestingly, given that the NDPR is not an Act of Parliament, questions have been raised regarding its efficacy and enforceability, and also with regards to the sufficiency of its scope.[93] In light of these shortcomings, a Data Protection Bill intended to succeed the NDPR was published by the Federal Government for comments in 2020. The Bill – similar to South Africa's POPI Act – provides for the requirement of consent from the data subject, a legitimate and explicit purpose for the processing of personal data, an adequacy decision for other jurisdictions etc. NITDA also released the Nigerian Cloud Computing Policy which promotes cross-border data transfers, but also requires that, where cloud service providers are contracted by Nigerian national institutions, this is under the condition that data is stored in a jurisdiction with equivalent data protection given by Nigeria.[94]

In relation to data localisation rules, the Mandatory Guidelines for Nigerian Content Development in Information and Communication Technology (the ICT Guidelines) – also enforced by NITDA – require telecommunication companies to host all subscribed and consumer data in Nigeria, and for data and information management firms to also host national/government data locally.[95] This was done with the aim to stimulate and increase indigenous innovation of information technology products and services for the development of the ICT industry. Separately, the Central Bank of Nigeria's 2011 Guidelines on Point of Sale (POS) Card Acceptance Services prescribe that infrastructure for payment processing should be located domestically. All point-of-sale and automated teller machine (ATM) domestic transactions need to be processed through local switches and are prohibited from being routed outside the country for processing.[96]

While data localisation rules can be beneficial, there is need for Nigeria to consider that, when these rules are enforced strictly, they can be protectionist, hindering cross-border data trade and serving as a non-tariff barrier. As a result, strict data localisation rules can constrict the full realisation of the economic benefits related to data-driven trade. This is an especially important consideration, given that article 15 of the AfCFTA's Protocol on Trade in Services only allows the enforcement of data localisation rules where they do not constitute 'arbitrary and unjustifiable discrimination.'[97] Therefore, much like South Africa, Nigeria must consider the possible incompatibility of strict data localisation rules with its regional commitments under the ECOWAS Supplementary Act (and the Malabo Convention if ratified), and also whether in the long-run, such measures would enable Nigeria to fully take advantage of the economic benefits it can get from data-driven trade. With the continued imposition of strict data localisation rules, Nigeria might also face challenges negotiating digital provisions with countries that defend the liberalisation of data flows, such as the US.

Kenya

Similar to South Africa and Nigeria, Kenya has also enforced data protection laws imbued with localisation requirements. Kenya's Data Protection Act of 2019 (KDPA) is the key legal instrument in relation to cross-border transfer of data, and to a greater extent follows the EU GDPR. Under the KDPA, the cross-border transfer of data is only allowed on the condition that the data controller or processor first provide evidence to the Data Commissioner that sufficient security and privacy safeguards are in place.[98] This includes the obligation placed on the data processor/controller of ensuring that, where the data transfer is necessary,[99] the destination country has equal data protection laws, and that the data subject (after being fully informed of any risks), consented to the cross-border transfer of their personal data.[100]

However, section 50 of the KDPA introduces some data localisation measures. Under this provision of the KDPA, the Cabinet Secretary has the authority to limit other types of personal or public data from being processed outside Kenya.[101] In addition, Kenya's proposed Data Protection Regulations of 2021 provide that, where data is being processed for any public service – including facilitating access to education, and revenue administration – this must be done through a local server and data centre in Kenya.[102] This means that any data processor/collector is prohibited from processing any personal data intended for a public service outside of Kenya or with foreign servers/data centres. These regulations highlight Kenya's priority to ensuring the privacy of its data subjects, while simultaneously – also similar to Kenya's ICT Policy – indicating the desire to grow the country's capacity to store and use its own data, including through the construction of central and regional data centres. In contrast to Nigeria, whose data localisation rules are underpinned by an economic interest, Kenya's objectives seem more driven by a need to provide maximum privacy for its data subjects.

Further to Kenya's domestic laws, the country also entered into the Economic Partnership Agreement between Kenya and the UK which provides guidelines stating that personal data may only be exchanged where the recipient country agrees to ensure a level of data protection that is equivalent to that of the source country.[103] This therefore establishes the need for adequacy prior to transfer, which is also echoed in Kenya's domestic regulations. Kenya is currently in the process of negotiating the US-Kenya FTA, whose negotiating objectives, according to the Office of the United States Trade Representative, indicate that the US will push for minimum barriers to cross-border data flows between the two countries.[104] Given Kenya's data localisation measures, there stands to be a clash between Kenya and the US on this matter.

Senegal

In contrast to South Africa, Kenya and Nigeria, Senegal seems to be employing a conditional transfer approach without any data localisation measures. Although it still presents some regulatory, implementation and enforcement gaps, Senegal's national data protection regime also closely follows the EU GDPR by prioritising the protection of the data owner. Senegal's Data Protection Act of 2008 (the 2008 DPA), which is currently in force, was modelled after the ECOWAS Supplementary Act which was heavily influenced by the EU data protection directive. In line with the ECOWAS Supplementary Act, Senegal's 2008 Act sets out fundamental rights for data

subjects such as requirements that the processing of personal data only be considered legitimate where the data owner/subject gives their consent to the processing of their data.[105] Where data is collected and processed, legitimate, explicit and specific reasons must exist, and any processing outside the confines of those purposes are not allowed.[106]

Senegal is currently considering the adoption of a new data protection law. Once in force, Senegal's proposed Personal Data Protection Bill of 2019 will provide more rights and protections to the data owner. For instance, the proposed Bill provides a narrower definition of 'consent', requiring that the data owner give clear permission for the use of their personal data through an affirmative action.[107] The data owner will also be allowed to revoke their consent to the processing of their data at any point. In addition, unlike the 2008 DPA, the 2019 Bill also will also oblige third-party subcontractors to comply with the law.[108]

In line with the EU approach, Senegal consistently requires that any cross-border data flows be made only with jurisdictions that ensure the same level of sufficient privacy and protection through their laws.[109] Where these securities do not exist, consent from the data owner/subject is required. However, Senegal does not currently have a system that grants adequacy agreements to jurisdictions with similar or satisfactory data protection regulations.[110] This suggests that data processing companies might have to seek permission for individual transfer of data into other jurisdictions, adding more responsibility to the Data Protection Commission to ensure compliance. While the lack of adequacy agreements is already problematic for Senegal, cross-border transfer of data might prove even more challenging for Senegal if countries agree on different adequacy standards to its own under the AfCFTA. This is especially pertinent because Senegal signed the EU Convention 108 which prioritises the 'right of privacy in relation to exchanges of personal data' and limits free flow of data where data protection legislation of a jurisdiction circumvents the Convention.[111]

3.3 Access to source code and technology transfer

In the digital age, the mandatory disclosure of source code and algorithms is one of the methods that policymakers have been using to facilitate the transfer of digital technologies for development purposes.[112] Source code refers to 'a collection of instructions typed into a computer which are processed and executed to … drive the software of the computer.'[113] Through the sharing and review of source codes, newer programming techniques are developed and software can be improved.[114] In particular, the flow of knowledge through source code disclosure from technologically advanced firms and countries creates opportunities for innovation, competitiveness and skills upgrading.[115]

The WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (the TRIPS Agreement)[116] laid the groundwork for the transfer of technology by obligating developed countries to provide incentives for technology transfer.[117] However, the TRIPS Agreement does not contain any specific provisions relating to the access to source code. Now, while source code may be protected under patents, trade secrets and/or copyright, the TRIPS Agreement does not contain any explicit prohibitions for countries to require the disclosure of source codes from foreign

companies. As a result, to address this concern, several countries such as the US, Singapore and the EU, have been pushing for the inclusion of intellectual property (IP) provisions that prohibit the mandatory disclosure of source code and algorithms in trade agreements.[118]

Developed countries such as the US and EU argue that the requirement to disclose source codes and algorithms serves as a market access barrier and a barrier to trade.[119] Therefore, such countries insist on the mandatory ban of source code disclosure. Some critics have also argued that the true rationale behind the ban on mandatory disclosure of source code and algorithms is largely based on the need to help firms retain a competitive advantage – creating market access for their technology-embedded products while protecting their IP.[120] For example, the ban in the USMCA aims to protect the IP and competitive advantage of its firms by prohibiting governments from setting as a pre-condition for market access, the provision of information about cryptography, including algorithms.[121] Similarly, the UK-Japan FTA also prohibits the mandatory disclosure by governments of source code, software and algorithms expressed in software.[122] Proponents of source code sharing argue that developed countries are guarding their competitive advantage by gatekeeping technological development – given that they already benefitted from source code sharing during the first phase of the digital revolution when source code was not protected by IP laws.[123]

However, source code is an integral contribution to the innovation and development of digital technologies. Prohibiting the sharing of source code may hinder the transfer of technology, limiting access to knowledge and constraining a country's ability to learn through imitation, and also to innovate, crafting distinct models in a global data value chain.[124] This challenge is even more acute for African countries that aim to harness the opportunities of digital technologies for economic development. Additionally, given that algorithms also give rise to public policy concerns such as discrimination, lack of fairness, transparency, and accountability,[125] advocates of artificial intelligence (AI) ethics argue that algorithms should be made transparent enough to be inspected, particularly when they inform decisions with questionable or negative repercussions.[126] IP policy therefore ought to be tailored to economic and social context, based on evidence, and informed by policy and development priorities. Taking a purely maximalist approach, as is being advanced in some fora, without appropriate exceptions and limitations, might hinder African countries from owning any significant IP rights or being relevant stakeholders in digital markets.[127] Issues around technology transfer, anti-competitive measures, barriers to compliance, and algorithmic accountability must be addressed, and the policies formulated in a manner that does not entrench the dominance of big firms at the expense of smaller ones.

Regional approaches to access to source code

Regionally, there have not yet been any specific development of rules relating to the mandatory disclosure of source code under institutions such as the African Regional Intellectual Property Organization (ARIPO)[128] or the Africa Intellectual Property Organization (OAPI).[129] Furthermore, as the analysis below indicates, because access to source code is relatively new, most African governments are yet to adopt domestic legislation that clearly defines their position and priorities

in relation to this issue. In particular, across this report's four focus countries, the development of regulation and policy on this issue is happening in a different manner and pace. For example, as explored below, while Nigeria's guidelines – though unimplemented – obligates multinational corporations to disclose the source code and algorithms of any software deployed in the country, South Africa's legislation currently limits mandatory disclosure to software procured by government. In contrast, Kenyan legislation promotes disclosure of source code, but does not specifically require it, while Senegal does not currently have legislation to this effect. A convergence of approaches exists among the four countries with regards to their interest in technology transfer and the policy space to request for disclosure of source code. However, ahead of the AfCFTA Phase II Negotiations, governments should consider if it might yet be premature to negotiate strict provisions on mandatory disclosure to source code in the AfCFTA. Therefore, AfCFTA members might find it useful to strive for regulatory co-operation in the meantime, while determining which regulatory approach best serves the region's developmental and economic interests.

South Africa

South Africa's domestic legislation requires the mandatory disclosure of source code, although this is currently limited to software used by government. Under South Africa's Policy on Free and Open Source Software Use for South African Government, as adopted by the Department of Public Service and Administration, only open-source software (OSS) is used in government projects.[130] Where this is not possible, the policy provides that justifications for this derogation must be provided. The policy also obligated the disclosure of the source code of every proprietary software that was in use before adoption of the policy in 2006.[131]

Generally, South Africa seems to be in support of technology transfer for economic development, especially in relation to science and technology. For example, South Africa's Intellectual Property Rights from Publicly Financed Research and Development Act of 2008 is intended to ensure that IP emanating from publicly financed research and development is commercialised and made available for the benefit of the South African public.[132] Building on this, the Department of Science and Technology[133] published a White Paper in 2019, framing South Africa's science, technology and innovation policy and reinforcing support for technology transfer, including the commercialisation of IP.[134]

Nigeria

In contrast, Nigeria's domestic policies favour the mandatory disclosure of source code and algorithms by imposing local content requirements for ICT. In particular, Nigeria's amended Guidelines for Nigerian Content Development in Information and Communication Technology (ICT guidelines) provide a number of guidelines for the treatment of source code. For example, under the ICT guidelines, for national security purposes, multinational companies are obligated to provide verifiable information about the origin, safety, source and operation of their software before it is deployed or sold in Nigeria.[135] In addition, Nigerian government ministries and departments at all three levels of governance – federal, state and local – are required to ensure the safety of all software used in the country, including through obtaining and reviewing the source code of the software from its parent company. Nigeria also ensures that there is technology transfer by insisting that, where the government requires the use of software, and no local Nigerian software

developer has capacity to provide it, any foreign company providing the software must work with a local Nigerian company.[136] Given that the functions expected of the local Nigerian company are installation and support, the disclosure of source codes and algorithms by the foreign software developer is therefore necessary to enable the local companies to fulfil their obligations. Although these ICT guidelines have not yet been implemented by Nigeria, they are a significant indicator of the country's position on this issue.

Kenya

Kenya currently only promotes the use of OSS in public administration. Under Kenya's National ICT Policy 2019, governments must use OSS, and opt for it whenever an alternative to proprietary software exists.[137] All software commissioned for development by the government must have its source code disclosed and made public for use by any other government agency.[138] The policy also provides that all government-procured software will have the source code listed in a public guide by government.

Senegal

While Senegal does not seem to have specific policies or laws relating to source code disclosure, the Senegalese public administration expressed interest in putting in place policies for free OSS.[139]

3.4 Intermediary liability

Rules relating to internet platforms' responsibility for content generated by users have been appearing in a number of trade agreements around the world, such as the US-Japan and the USMCA. These rules determine whether and how internet platforms that serve as intermediaries[140] should be legally responsible for online harms and violation of rights caused by third-party content that they host or transmit.

Figure 3: Approaches to intermediary liability

Actual knowledge approach	Notice and takedown approach	Mere conduit approach	US Digital Millennium Copyright Act	Malabo Convention
• Intermediaries are only responsible for content they were aware of	• Intermediaries must take down content as soon as they are made aware of its illegal nature	• Intermediaries are protected where their conduct was automatic and passive in nature	• Intermediaries are indemnified from liability from illegal content, and are protected from liability that might result from trying to moderate third-party content	• African member states are to criminalise the hosting, dissemination and transmission of images or representations which translate to child pornography, as well as racist or xenophobic content
• eg. Australia, Japan, India	• eg. New Zealand, UK	• eg. EU		

As shown in Figure 3, countries have adopted different approaches to intermediary liability. Some countries have adopted legislation that reflects the 'actual knowledge' model where they hold intermediaries accountable for content that they are only aware of. For example, in their domestic legislation, Australia, Japan and India have adopted this model, absolving intermediaries of any liability where they were unaware of the nature of the content, and only holding them responsible where they failed to remove or disable access to the content on acquiring knowledge that it infringes on the rights of others.[142] In contrast, other countries such as New Zealand and the UK have been opting for the 'notice and takedown' model where – as a way to escape liability – intermediaries are required to take down any unlawful content on their platforms as soon as it is reported to them. While this model protects intermediaries from the burden of proactively controlling and ensuring the legal suitability of every piece of content prior to it being posted, it has also been criticised for incentivising platforms to take down any reported content without necessarily investigating whether it infringes the law.[143] The 'mere conduit' is also a model that is being employed by jurisdictions such as the EU. This approach protects intermediaries from liability in instances where their activity was automatic and passive in nature – for example, services such as caching and hosting.[144]

Interestingly, as shown in Figure 3, the US adopts a slightly different model to intermediary liability which contains elements of all three approaches.[145] Under US law, intermediaries are indemnified from any legal consequences arising from the illegal content by third-party users, and are also protected from liability that might result from trying to moderate third-party content.[146] This means that intermediaries are immune from liability whether they distribute illegal third-party content or unjustly remove any third-party content which may or may not be illegal. Critics of this approach have argued that it is too broad and therefore shields intermediaries from responsibility where their platforms result in a direct or indirect infringement of the rights of internet users.[147] Furthermore, the US also seems to have influenced some of its trading partners to adopt its approach to intermediary liability in its trade agreements – for example, language that closely mirrors US law on this subject appears in the US-Japan Digital Trade Agreement, as well as the USMCA.[148]

Regional approaches to intermediary liability

In contrast to all the models explained above, the African Union's Malabo Convention adopted a completely different approach, advocating for the 'intermediary responsibility' model. Under the Malabo Convention, African member states are to criminalise the hosting, dissemination and transmission of images or representations which translate to child pornography, as well as racist or xenophobic content.[149] Critics of the Malabo Convention have argued that it is too strict and therefore might have the effect of stifling digital business as well as free speech online. It is also significant to note – as discussed below – that all four of this report's focus countries have also adopted regulatory models that diverge from the Malabo Convention. In particular, while each of the four countries' regulatory approaches differ, there is a common interest not to place too much liability on the intermediary, unlike the responsibility the Convention imputes on intermediaries. However, regardless of this seemingly similar interest, all four countries maintain diverging regulatory approaches.

It is therefore clear that the regulation of content and intermediary liability is complex and needs to be carried out in a balanced manner. While 'fake news', misinformation, and hate speech pose threats to internet users, experts consider that overly broad or misaligned content regulation is also capable of infringing users' rights.[150] For example, some liability models give incentives for platforms to use filtering tools and adopt review procedures that may violate human rights, such as censoring legitimate speech. As trade agreements increasingly include provisions regulating internet content and liability of intermediaries, trade policy should strive to achieve a balance between these objectives.[151] It is therefore vital that, in the build-up to the AfCFTA's Phase II Negotiations, countries carefully consider the implications of all the models discussed, in light of their social, political and economic priorities and interests. AfCFTA members might also need to determine if harmonisation would achieve their policy and economic goals, and also whether the AfCFTA is the best platform for addressing these issues.

South Africa

Currently, South Africa's approach to intermediary liability is a hybrid one, combining different elements from the models shown in Figure 3. Under South Africa's Electronic Communications and Transactions Act of 2002 (the ECT Act), intermediaries are only indemnified from liability in instances where they transmitted, cached, stored, or hosted unlawful content without the knowledge of the nature of the such content.[152] Borrowing from the 'actual knowledge' model, the indemnity is also offered on the condition that intermediaries do not modify, participate in the creation of, or in any way select the receiver of the content.[153] The ECT Act however, also includes a 'notice and takedown' provision, requiring intermediaries to remove, disable access, or halt transmission where they are notified that content is unlawful.[154] However, similar to the US model, where there is wrongful takedown of content, South African law protects intermediaries, imputing liability instead to the individual who submitted the notice, given that they knowingly misrepresented the facts.[155] South Africa's legislation differs from the US approach by providing that intermediaries can only benefit from these safe harbour provisions if: they are members of an industry representative which is registered with the Department of Communications; and they adopt and implement the industry representative's code of conduct. As a result, the industry representative is given the authority to define the specific takedown procedures.[156] South African policymakers deem this model to be the most effective and crucial in terms of making internet services more publicly available.[157] As mentioned above, South Africa's position also differs from that provided for under the Malabo Convention.[158]

Nigeria

While Nigeria currently has no explicit laws addressing intermediary liability, the Nigerian Communications Commission published a set of guidelines for the provision of internet services which included both a notice and takedown mechanism, as well as safe harbour provisions for internet service providers that act as content intermediaries.[159] In line with the 'notice and takedown' model, the Commission's guidelines require that internet service providers disconnect subscribers or take down content once they are made aware that the activity or content is in contravention of the guidelines or other applicable laws.[160] It is important to note that there is currently no publicly available case law indicating if, and how the guidelines have been enforced.

However, Nigeria can be argued to have used a version of intermediary responsibility by imposing a ban on Twitter[161] in June 2021 on the basis that it had been used to 'organise, co-ordinate and execute' illegal content.[162] Following the Twitter ban, the federal government issued a directive requiring that social media and over-the-top platforms (a service that allows users to deliver pre-recorded and live-streamed content) operating in the country register with the Corporate Affairs Commission and obtain a licence from the National Broadcasting Commission.[163] These events suggest Nigeria's preference for strict liability on content that affects 'matters of national interest'.

Kenya

Kenya's approach to intermediary liability differs from South Africa and Nigeria. Kenya's Copyright (Amendment) Act 20 of 2019 and the proposed Intellectual Property Bill of 2020[164] provide the copyright protection of works such as computer programs, audio and audio-visual content, and works of literature. Borrowing heavily from the US Digital Millennium Copyright Act, the Bill proposes four safe harbours: conduit, caching, hosting, and information location.[165] Copyright owners can issue a takedown notice to a service provider, where non-compliance can result in imprisonment or a fine for the service provider. It must be noted however, that these provisions apply to the copyright of works such as 'computer programs, audio and visual content' etc.; in the context of Kenya's IP law. As a result, contrasted to South Africa and Nigeria, the notice of takedown provisions cannot be broadly applied to intermediaries.

However, Kenya's Computer Misuse and Cybercrimes Act of 2018 criminalises the publication of false data or news, cyber-harassment, wrongful distribution of obscene or intimate messages, computer fraud, child pornography and cyber-squatting.[166] The obligation imposed on users is to ensure the accuracy of content before posting it online, with infringement resulting in heavy penalties such as fines or prison time. However, digital rights activists have indicated that some of its provisions lack definitional clarity. For example, the Act criminalises the publication of 'false information', without clearly defining what constitutes 'fake news'. Given various issues, including the ambiguity in what qualifies as an offense, following its release, the Bloggers Association of Kenya filed a petition challenging it and arguing that it was unconstitutional because it limited users' rights to freedom of speech and access to information.[167]

Senegal

Senegal currently limits liability on intermediaries and places no specific obligations on them to monitor content.[168] According to Senegal's Law on Electronic Transactions, intermediaries cannot be held liable for storing content where they were unaware that the content was of an illicit nature.[169] However, Senegal also requires that, where content that is stored on intermediary platforms consists of 'crimes against humanity, incitement to racial hatred and child pornography,' intermediaries must inform the authorities.[170] Senegal's Law on Electronic Transactions also requires intermediaries to follow a notice and takedown regime in addition to ensuring that mechanisms are in place to remove or prevent access to unlawful content.[171] As mentioned above, there is a discrepancy between Senegal's indemnity of intermediaries under its domestic law, in comparison to the stricter rules of intermediary responsibility under the Malabo Convention which Senegal already ratified.[172] For example, where Senegal precludes liability from intermediaries for

unknowingly storing illicit content, the Malabo Convention requires that they face criminal charges. Now, although Senegal's position on intermediary liability is unclear because of this discrepancy, Senegal's ratification of the Malabo Convention legally requires it to revise its domestic law to reflect rules on intermediary responsibility.

3.5 Customs duties on electronic transmissions

As digital trade advances, governments have also been looking into viable ways of revenue collection that simultaneously allow for economic growth. In this regard, countries – particularly developing and developed – have been divided on whether or not customs duties on electronic transmissions should be imposed. While several trade agreements, such as the Singapore-Australia FTA, the Japan-Switzerland Economic Partnership Agreement and the New Zealand-Taiwan FTA have included provisions on the prohibition of customs duties, most African countries at the WTO have adopted a firm stance supporting the imposition of customs duties on electronic transmissions.

In 1998, WTO members agreed to a two-year moratorium (WTO moratorium) prohibiting countries from imposing custom duties on electronic transmissions, with a view to encouraging this new aspect of global trade. Though members have maintained the WTO moratorium, it is a contentious issue for several reasons. Members disagree on the definition of 'electronic transmissions', leaving the scope of electronic transmissions unclear. A 2016 study by the WTO secretariat narrowly characterised electronic transmissions as 'digitisable goods' that include 'cinematograph film, books, newspapers and journals, other printed matter, video games, computer software, musical records, tapes and other sound or similar recordings, and other recorded media.'[173] This understanding of electronic transmissions – covering content that is transmitted electronically – is a definition shared by some WTO members (mostly developed country members).[174] In contrast, other WTO members disagree with this definition, viewing electronic transmissions more broadly as covering the carrier medium,[175] or 'any physical object capable of storing the digital codes that form a digital product capable of storing the digital codes that form a digital product by any method now known or later developed, reproduced, or communicated, directly or indirectly, and includes an optical medium, a floppy disk and a magnetic tape.'[176]

WTO members also disagree on whether or not customs duties on electronic transmissions should be prohibited permanently. Proposals in favour of the moratorium have cited benefits such as the improvement of consumer access to new products and services through the elimination of burdensome customs duties.[177] However, questions remain as to whether the gains from such arrangements would be evenly distributed across countries. Developing countries are opposed to permanently adopting the ban viewing it as 'granting the digitally advanced countries duty-free access to [their] markets'.[178] For example, the African Group at the WTO is of the position that disallowing customs duties on electronic transmissions would be detrimental to developing countries and would result in significant revenue losses.[179] In support of this, a 2019 UNCTAD report

found that, for Sub-Saharan African countries in particular, a potential loss in tariff revenue was likely to be twice that of WTO developed countries if the moratorium was permanently adopted.[180] However, in the context of total government revenues, this has been argued to be very small, and concentrated only in a few of the larger developing countries.[181]

South Africa

South Africa does not currently have any legislation on customs duties on electronic transmissions. However, the country expressed concerns over the scope of the WTO moratorium and the consequent tariff revenue losses, as well as the negative impact the moratorium might have on digital-led economic growth in developing countries.[182] This concern was based on the digital divide that exists between developing and developed countries, which will allow developed countries to benefit more from the moratorium.[183]

Nigeria

Similar to South Africa, Nigeria does not currently have any direct laws on the imposition of customs duties on electronic transmissions.

Kenya

Kenya also does not currently have any direct laws on the imposition of customs duties on electronic transmissions. However, it is also a part of the African Group of countries at the WTO who are opposing the permanent adoption of the moratorium. In light of Kenya's position, it remains to be seen whether the country will uphold this position in the context of the proposed US-Kenya FTA. While yet to be concluded, experts argue that the US will seek prohibition of such tariffs, so as not to disadvantage US-owned companies, with negative implications for the much smaller local start-ups.[184]

Senegal

Senegal, together with the WTO's African Group, firmly opposed the permanent adoption of the WTO moratorium which prohibits the imposition of customs duties on electronic transmissions. According to this position, disallowing customs duties on electronic transmissions would be detrimental to developing countries and would result in significant revenue losses.[185]

4. Conclusion

This study highlights the divergencies that exist in how four AfCFTA members are regulating five specific policy issues related to digital trade. The study shows that, in some specific policy areas (such as the regulation of e-signatures and intermediary liability), all four countries adopt mainly different approaches, even though they consist of similar elements. For example, although all four countries recognise e-signatures as valid, they differ in the types of e-signatures legally recognised, including when such signatures were considered valid. In terms of intermediary liability, South Africa, Nigeria and Senegal all have laws that provide indemnity for intermediaries; however, this is based on different criteria.

The study also highlights that, in some policy areas (such as mandatory disclosure of source code), although the four countries share a common interest, divergencies exist around the level of regulation, implementation, and enforcement of the rules. In particular, Nigeria is the only country out of the four that imposes requirements for multinational enterprises to disclose their source code before any software is dispatched in Nigeria. The other three countries have adopted rules that either require or promote the sharing of source code for public use. It is also important to note that, in some policy areas (such as cross-border data flows), divergencies also exist between the domestic and regional laws. For example, while instruments such as the ECOWAS Supplementary Act primarily borrow from the EU GDPR, Nigeria (which is an ECOWAS member) still imposes strict data localisation rules.

Given that the intention of the AfCFTA Phase II Negotiations is primarily to work toward harmonisation of specific regulations to improve intra-African trade, and also promote the region's international trade, it is vital for AfCFTA members to reflect on the differences in their national policies and domestic regulatory approaches. An outlook on these divergencies will allow AfCFTA members to weigh the costs of such divergencies, and also to determine whether harmonisation is necessary, and where it can be achieved efficiently for key issues. Considering these issues will also highlight where there is potential for interoperability, allowing members to consider where AfCFTA is the appropriate platform for either harmonisation or interoperability.

Endnotes

1 This is with the exception of Senegal whose current laws were modelled after the EU Data Protection Directive, and its upcoming laws modelled after the GDPR.

2 For the purposes of this report, digital trade is defined as digitally enabled transactions comprising the exchange of goods and services that can either be digitally or physically delivered, and involving consumers, firms, and governments. It is closely linked to e-commerce defined by the WTO as the production, distribution, marketing, sale or delivery of goods and services by electronic means in transactions involving enterprises, households, individuals, governments and other public or private organisations.

3 For a detailed discussion on the definition of digital trade, see Emily Jones et al. (2021), *The UK and Digital Trade: Which Way Forward?* Blavatnik School of Government. Available at: https://www.bsg.ox.ac.uk/research/publications/uk-and-digital-trade-which-way-forward.

4 Susan Aaronson and Patrick Leblond (2018), Another Digital Divide: The Rise of Data Realms and Its Implications for the WTO, *Journal of International Economic Law 1.*

5 Bai Gao and Yi Ru (2021), Industrial Policy and Competitive Advantage: A Comparative Study of the Cloud Computing Industry in Hangzhou and Shenzhen, in Baark, Hofman and Qian (eds) *Innovation and China's Global Emergence,* National University Press of Singapore, 232 Available at: epress.nus.sg/innovationandchina/InnovationandChinasGlobalEmergence.pdf#page=242.

6 Faith Tigere (2021), *The WTO and Africa: The State of Play and Key Priorities Going Forward,* SAIIA, Policy Briefing, 243. Available at: https://saiia.org.za/research/the-wto-and-africa-the-state-of-play-and-key-priorities-going-forward.

7 OECD (2021), *Members of the OECD/G20 Inclusive Framework on BEPS*. Available at: https://www.oecd.org/tax/beps/inclusive-framework-on-beps-composition.pdf.

8 Jonathan Kamoga, 13 Countries Urged to Ratify Trade Deal, *The EastAfrican* (16 November 2021) Available at: https://www.theeastafrican.co.ke/tea/business/13-countries-urged-to-ratify-trade-deal-3620340.

9 Mira Burri and Rodrigo Polanco (2020), Digital Trade Provisions in Preferential Trade Agreements: Introducing a New Dataset, *Journal of International Economic Law*, Volume 23, 187, 193.

10 Burri and Polanco (n 9).

11 Lillyana Daza Jaller and Martin Molinuevo (2020), *Digital Trade in MENA: Regulatory Readiness Assessment,* World Bank Group Policy Research Working Paper 6. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/33521/Digital-Trade-in-MENA-Regulatory-Readiness-Assessment.pdf.

12 Jaller and Molinuevo (n 11) 8.

13 Taku Nemoto and Javier López González (2021) Digital Trade Inventory: Rules, Standards and Principles, OECD, Available at: https://www.oecd-ilibrary.org/docserver/9a9821e0-en.pdf.

14 Minyan Wang (2006), *A Review of Electronic Signatures Regulations: Do They Facilitate or Impede International Electronic Commerce?* Centre for Commercial Law Studies, 548, 548.

15 Electronic signatures being defined as 'symbols or other data in digital form attached to an electronically transmitted document as verification of the sender's intent to sign the document'; and digital signatures as 'a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate' – both according to the Oxford Dictionary.

16 Wang (n 14) 548.

17 Ibid.

18 Wang (n 14) 549.

19 Ibid.

20 Wang (n 14) 549; Emily Jones et al. (2021), *The UK and Digital Trade: Which Way Forward?* BSG Working Paper Series 41. Available at: https://www.bsg.ox.ac.uk/sites/default/files/2021-02/BSG-WP-2021-038_0.pdf.

21 Jones et al. (n 20) 40.

22 Ibid.

23 Wang (n 14) 549. ; Jones et al. (n 20) 41.

24 UNCTAD (2021), E-Transactions Legislation Worldwide (UNCTAD Cyberlaw Tracker) Available at: https://unctad.org/page/e-transactions-legislation-worldwide.

25 World Economic Forum (2017). *Making Deals in Cyberspace: What's the Problem?*

26 Electronic Communications and Transactions Act 2002.

27 Karishma Banga, Jamie Macleod and Max Mendez-Parra (2021), *Digital Trade Provisions in the AfCFTA: What Can We Learn from South–South Trade Agreements?* 28.

28 Electronic Communications and Transactions Act 2002.

29 Supplementary Act on Personal Data Protection within ECOWAS 2010 s 34; Cybercrimes (Prohibition, Prevention, Etc.) Act of Nigeria, 2015 s 17(1)(a).

30 Evidence Act of Nigeria, 2011 s 93(3).

31 A signature that meets all the following requirements: (i) it is uniquely linked to the signatory; (ii) it is capable of identifying the signatory; (iii) it is created using means that the signatory can maintain under his sole control; and, (iv) it is linked to the data to which it relates in such a manner that any subsequent change to the data is detectable.

32 The Business Laws (Amendment) of Kenya 2020.

33 Ibid.

34 William Maema and Imelda Anika (2020), What It Means to Use Electronic Signatures, *Insights*, DLA Piper Africa. Available at: https://www.dlapiperafrica.com/en/kenya/insights/2020/what-it-means-to-use-electronic-signatures.html.

35 Loi no. 2008-08 sur Les Transactions Electroniques 2008.

36 This includes the public-private company GAINDE 2000, which operate the Senegalese single window and introduced a paperless trading environment in Senegal.

37 UNECE (2016), A Road Towards Paperless Trade: Senegal's Experience, *Trade Facilitation Implementation Guide: Case Stories*, 1. Available at: https://tfig.unece.org/cases/Senegal.pdf.

38 Alfred Filani (2020), E-Commerce and Enforcement of Consumer Rights in Nigeria: Issues, Prospects and Challenges, *Journal of Law and Judicial System*, Volume 3, Issue 1, 1.

39 Tunde Ibidapo-Obe (2011), *Online Consumer Protection in E-Commerce Transactions in Nigeria: An Analysis*, University of Sussex. Available at: https://www.researchgate.net/publication/314459028_Online_Consumer_Protection_in_E-Commerce_Transactions_in_Nigeria_An_Analysis.

40 Jones et al. (n 20) 41.

41 Karishma Banga et al. (2021) *E-Commerce in Preferential Trade Agreements: Implications for African Firms and the AfCFTA*, ODI, 15. Available at: https://cdn.odi.org/media/documents/e-commerce_in_preferential_trade_agreements_report.pdf; Despoina Mantzari and Ioannis Lianos, *The Global Governance of Online Consumer Protection and E-Commerce: Building Trust*, World Economic Forum (2019) 19. Available at: www3.weforum.org/docs/WEF_consumer_protection.pdf; Jones et al. (n 20).

42 Loly Gaitan and Julien Grollier (2020), *Electronic Commerce in Trade Agreements: Experiences of Small Developing Countries*, CUTS International, 26. Available at: www.cuts-geneva.org/pdf/eAfCFTA-Study-E-Commerce_Provisions_in_RTAs.pdf.

43 Gaitan and Grollier (n 42) 27.

44 Electronic Transactions and Electronic Commerce: Southern African Development Community (SADC) Model Law 2013 pt IV.

45 Banga et al. (n 41).

46 Electronic Communications and Transactions Act 2002.

47 Ibid.

48 Electronic Communications and Transactions Act 2002.

49 Federal Competition and Consumer Protection Act of Nigeria 2018.

50 Ifeoluwa Adeyemo, Nigeria Consumer Council Sets New Guidelines to Protect E-Commerce Consumers, *Nigeria Premium Times* (15 March 2018) Available at: https://www.premiumtimesng.com/business/business-news/261961-nigeria-consumer-council-sets-new-guidelines-to-protect-e-commerce-consumers.html.

51 Adeyemo (n 50).

52 Consumer Protection Act of Kenya 2012.

53 Ibid. s 2.

54 Ibid. s 31,32,33.

[55] Decret Relatif au Commerce Electronique pris pour l'application de la loi no. 2008 sur les transactions electroniques 2008 s 10.

[56] Ibid. s 15.

[57] Ibid.

[58] Taku Nemoto and Javier López González (2021), *Digital Trade Inventory: Rules, Standards and Principles*, OECD, 8. Available at: https://www.oecd-ilibrary.org/docserver/9a9821e0-en.pdf.

[59] Anupam Chander and Martina Ferracane (2019) Regulating Cross-Border Data Flows – Domestic Good Practices, in *Exploring International Data Flow Governance: Platform for Shaping the Future of Trade and Global Economic Interdependence*, World Economic Forum, 7. Available at: https://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf.

[60] Franscesca Casalini and Lopez Gonzalez Javier (2019) *Trade and Cross-Border Data Flows*, OECD Trade Policy Papers, No. 220, OECD, 5. Available at: https://www.sipotra.it/old/wp-content/uploads/2019/01/Trade-and-Cross-Border-Data-Flows.pdf.

[61] World Bank (2021), *World Development Report: Data for Better Lives*. Available at: https://www.worldbank.org/en/publication/wdr2021.

[62] World Bank (n 61) 238–241.

[63] Shaffer Gregory (2002), *Managing U.S-EU Trade Relations through Mutual Recognition and Safe Harbor Agreements: "New" and "Global" Approaches to Transatlantic Economic Governance?* European University Institute Working Papers, Robert Schuman Centre for Advanced Studies, 22–23.

[64] Reyes Carla (2011) WTO-Compliant Protection of Fundamental Rights: Lessons From the EU Privacy Directive, *Melbourne Journal of International Law*, Volume 12, 6. Available at: https://law.unimelb.edu.au/__data/assets/pdf_file/0010/1686934/Reyes.pdf; Yakovleva Svetlana Irion Kristina (2020) Pitching Trade Against Privacy: Reconciling EU Governance of Personal Data Flows With External Trade, *International Data Privacy Law*, Volume 10, Issue 3, Oxford University Press, 6.

[65] Reyes Carla (n 64) 6.

[66] Alexander Beyleveld (2021) *Data Localisation in Kenya, Nigeria and South Africa: Regulatory Frameworks, Economic Implications and Foreign Direct Investment*, Policy Brief 07, Mandela Institute. Available at: https://www.wits.ac.za/media/wits-university/faculties-and-schools/commerce-law-and-management/research-entities/mandela-institute/documents/research-publications/800553%20PB7%20Data%20localisation%20and%20FDI%20in%20Kenya%2001A.pdf

[67] Wu T (2006) The World Trade Law of Censorship and Internet Filtering, *Chicago Journal of International Law*, Issue no. 7, 281.

[68] Martina Ferracane (2018) *South Africa and Data Flows*, GEGAfrica Discussion Paper, April 2018. Available at: https://www.gegafrica.org/item/651-south-africa-and-data-flows-how-to-fully-exploit-the-potential-of-the-digital-economy.

[69] Shanelle van der Berg (2021) *Data Protection in South Africa: The Potential Impact of Data Localisation on South Africa's Project of Sustainable Development*, Mandela Institute Policy Brief Series 6.

70 Pathways for Prosperity Commission (2019) Digital Diplomacy: Technology Governance for Developing Countries, University of Oxford, 35. Available at: https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2019-10/Digital-Diplomacy.pdf.

71 Christopher Foster and Shamel Azmeh (2020), Latecomer Economies and National Digital Policy: An Industrial Policy Perspective, *Journal of Development Studies* 56 (2), 1247, 1259.

72 Institute of International Finance (2020), *Data Localisation: Costs, Tradeoffs, and Impacts Across the Economy*. Available at: https://www.iif.com/Portals/0/Files/content/Innovation/12_22_2020_data_localization.pdf.

73 Institute of International Finance (n 72) 5.

74 The African Union (2020) *The Digital Transformation Strategy for Africa (2020–2030).*

75 African Union Convention on Cyber Security and Personal Data Protection 2014.

76 African Union (2020) *African Union Convention on Cyber Security and Personal Data Protection – Status List.*

77 Koliw Majam and Janny Montinat (2021) *Privacy and Personal Data Protection in Africa: Advocacy Toolkit*, African Declaration on Internet Rights and Freedoms Coalition, 37. Available at: https://www.apc.org/en/pubs/privacy-and-personal-data-protection-africa-advocacy-toolkit.

78 Majam and Montinat (n 77) 36.

79 Sylla, A, Ford-Cox, A (2019) *Overview of data protection laws in Africa*. Lexology. Available at: https://www.lexology.com/library/detail.aspx?g=82196d1c-2faa-43c2-983b-be3b0f1747f2

80 Moritz Hennemann Patricia Boshe (forthcoming), African Data Protection Laws, Global Privacy Law Review, 35. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3947664

81 Patricia Boshe (n 80) 35.

82 UNCTAD (2021) *Digital Economy Report 2021, xv*. Available at: https://unctad.org/webflyer/digital-economy-report-2021.

83 Michael Pisa and Ugonma Nwako (2021) *Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development: Roundtable Summary*, Centre for Global Development, 2. Available at: https://www.cgdev.org/sites/default/files/are-current-models-data-protection-fit-purpose-understanding-consequences-economic.pdf.

84 Most of the substantial provisions entered into force on 1 July 2020, although some rules only commenced on 30 June 2021.

85 Although largely similar to the EU GDPR, South Africa's POPI Act is only applicable to responsible parties who are either domiciled in South Africa or make use of automated or non-automated means in South Africa.

86 Electronic Communications Act: Draft National Policy on Data and Cloud 2021; Global Data Alliance, Comments to the Republic of South Africa on the Proposed Data and Cloud Policy (April 2021). Available at: https://www.globaldataalliance.org/downloads/05122021gdasafrdatacloud.pdf.

87 Electronic Communications Act: Draft National Policy on Data and Cloud.

88 van der Berg (n 69) 3.

89 Nigeria Data Protection Regulation 2019.

90 Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) 2019 s 2.11.

91 Ibid. s 2.10.

92 Nigeria Data Protection Regulation 2019.

93 Kenneth Erikume and Wunmi Adetokunbo-Ajayi (2020) The NDPR and the Data Protection Bill 2020, pwc. Available at: https://www.pwc.com/ng/en/publications/data-protection-bill-2020.html.

94 Nigerian Cloud Computing Policy 2019.

95 Guidelines for Nigerian Content Development in Information and Communication Technology (ICT).

96 Central Bank of Nigeria (2011). Guideline on Point of Sale (POS) Card Acceptance Service. Section 4.4.8.

97 AfCFTA Protocol on Trade in Services.

98 Kenya Data Protection Act 2019; Data Protection (General) Regulations of Kenya 2021.

99 Necessary is defined as: (i) for the performance of a contract between the data subject and the data controller or data processor or implementation of precontractual measures taken at the data subject's request; (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person; (iii) for any matter of public interest; (iv) for the establishment, exercise or defence of a legal claim; (v) to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or (vi) 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.

100 Kenya Data Protection Act 2019.

101 Kenya Data Protection Act 2019.

102 Kenya Data Protection (General) Regulations 2021.

103 See Economic Partnership Agreement between the United Kingdom of Great Britain and Northern Ireland, of the one part, and the Republic of Kenya, a member of the East African Community, of the other part, Protocol 2 Article 10 and 13

104 Office of the United States Trade Representative (2020) United States-Kenya Negotiations: Summary of Specific Negotiating Objectives, 7. Available at: https://ustr.gov/sites/default/files/Summary_of_U.S.-Kenya_Negotiating_Objectives.pdf.

105 Loi portant sur la Protection des donnees a caractere personnel 2008.

106 Ibid.

107 Loi sur la Protection des Donnes Personnelles 2019 s 8.

108 Loi sur la Protection des Donnes Personnelles 2019.

109 Loi portant sur la Protection des donnees a caractere personnel 2008; Loi sur la Protection des Donnes Personnelles 2019.

110 Given the current gaps in its regime, Senegal has also not been granted an adequacy decision by the EU.

111 Council of Europe (2021), Convention 108 and Protocols. Available at: https://www.coe.int/en/web/data-protection/convention108-and-protocol.

112 WTO (2017) *Some Preliminary Implications of WTO Source Code Proposal*, Third World Network Briefings, 4. Available at: https://twn.my/MC11/briefings/BP4.pdf.

113 Muhammad Irfan (2019) *Data Flows, Data Localisation, Source Code: Issues, Regulations and Trade Agreements*, CUTS International, 16. Available at: www.cuts-geneva.org/pdf/WTOSSEA2018-Study-Data_Flows_Localisation_Source_Code.pdf.

114 Irfan (n 113) 17.

115 UNCTAD (2014) *Studies in Technology Transfer: Selected Cases from Argentina, China, South Africa and Taiwan Province of China*, 2. Available at: https://unctad.org/system/files/official-document/dtlstict2013d7_en.pdf.

116 TRIPS sets minimum standards for various elements of IP, including patents, trademarks, copyright, and trade secrets.

117 WTO (1994) Agreement on Trade-Related Aspects of Intellectual Property Rights 1994 s 66.2. Available at: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm.

118 WTO (2019) Joint Statement on Electronic Commerce: Communication from Singapore. INF/ECOM/25. Available at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/25.pdf&Open=True.

119 Irfan (n 113) 17.

120 Jones et al. (n 3).

121 United States-Mexico-Canada Agreement 2018.

122 Japan-UK Comprehensive Economic Partnership Agreement 2020.

123 Irfan (n 113) 16.

124 Valente, MG (2020) *Digital Technologies and Copyright: International Trends and Implications for Developing Countries*, Digital Pathways at Oxford Paper Series; No. 1. Available at: https://pathwayscommission.bsg.ox.ac.uk/Mariana-Valente-digital-technologies-and-copyright.

125 Lee Raine and Janna Anderson (2017), *Code-Dependent: Pros and Cons of the Algorithm Age*, Pew Research Center. Available at: https://www.pewresearch.org/internet/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age.

126 Sandra Wachter, Brent Mittelstadt and Chris Russell (2018) Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR, *Harvard Journal of Law and Technology* Volume 31, 841.

127 Valente (n 124).

128 ARIPO was established through the 1976 Lusaka Agreement to promote co-operation in industrial property among member states to achieve technological advancement for economic and industrial development. It achieves this through, (among other actions): (i) promoting the harmonisation and development of the industrial property laws, appropriate to the needs of its members; (ii) establishing such common services or organs as necessary for the co-ordination and; (iii) promoting the exchange of ideas and experience, research and studies relating to industrial property matters.

129 OAPI was established in March 1977 through the Bangui Agreement with the aim of encouraging member states to collaborate, build networks and share common resources with regards to intellectual property. The Bangui Agreement serves as a national law for each of the 17 states, which are primarily from Francophone Africa.

130 Policy on Free and Open Source Software Use for South African Government 2006.

131 Ibid.

132 Intellectual Property Rights from Publicly Financed Research and Development Act: Regulations 2008; Nazeem Mustapha and Gerard Ralphs (2021) Effectiveness of Technology Transfer in Public Research Institutions in South Africa: A Critical Review of National Indicators and Implications for Future Measurement, *African Journal of Science, Technology, Innovation and Development*, 1.

133 The National Intellectual Property Management Office established by the Intellectual Property Rights from Publicly Financed Research and Development Act 2008, and also part of the Department of Science and Technology, is responsible for enforcing these provisions.

134 Department of Science and Technology, Republic of South Africa (2019) *White Paper on Science, Technology and Innovation 2019*. Available at: https://www.dst.gov.za/images/2019/White_paper_web_copyv1.pdf.

135 Guidelines for Nigerian Content Development in Information and Communication Technology (ICT).

136 Ibid.

137 Kenya National ICT Policy 2019.

138 Ibid.

139 Mawaki Chango and Sadio Insa (2020) *Evaluation Du Développement de l'Internet Au Sénégal: Utilisation Des Indicateurs ROAM-X de l'universalité de l'Internet de l'UNESCO*, UNESCO, 68. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000374740.

140 Internet platforms are considered intermediaries where their services include receiving, storing, and transmitting user-generated content instead of the platform publishing content themselves (Facebook, YouTube, and Twitter fall under this category).

141 Ashley Johnson and Daniel Castro (2021) *How Other Countries Have Dealt with Intermediary Liability*, Information Technology & Innovation Foundation, 1. Available at: https://itif.org/sites/default/files/2021-section-230-report-4.pdf.

142 Australia's Broadcasting Services Act 1992; India's Information Technology Act 2000; Japan's Provider Liability Limitation Act 2001.

143 Johnson and Castro (n 141) 2.

144 Johnson and Castro (n 141) 4.

145 At the time of writing, the US was considering reforming s.230 on intermediary liability.

146 US Communications Decency Act – Title V of the Telecommunications Act 1996; US The Digital Millennium Copyright Act 1998; Johnson and Castro (n 141) 7.

147 Ashley Johnson and Daniel Castro (2021) *Fact Checking the Critiques of Section 230: What Are the Real Problems?* Information Technology & Innovation Foundation, 1. Available at: https://itif.org/sites/default/files/2021-230-report-3.pdf.

148 Johnson and Castro (n 141) 7; Johnson and Castro (n 147).

149 African Union Convention on Cyber Security and Personal Data Protection.

150 Global Network Initiative (2020) Trends in Content Regulation in Africa and Beyond, Report from the GNI Session at FIFAfrica. Available at: https://medium.com/global-network-initiative-collection/trends-in-content-regulation-in-africa-and-beyond-report-from-the-gni-session-at-fifafrica-6c6a6e757f7e.

151 Jones et al. (n 3).

152 Electronic Communications and Transactions Act 2002 ch XI.

153 Ibid.

154 Ibid.

155 Ibid.

156 Nicolo Zingales (2020) Intermediary Liability in Africa: Looking Back, Moving Forward?, in Giancarlo Frosio (Ed) *Oxford Handbook of Online Intermediary Liability*. Available at: https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198837138.001.0001/oxfordhb-9780198837138-e-11.

157 Alex Comninos (2012) *Intermediary Liability in South Africa*, Association for Progressive Communications, 5. Available at: https://www.apc.org/sites/default/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf.

158 African Union Convention on Cyber Security and Personal Data Protection 9; Zingales (n 156).

159 Guidelines for the Provision of Internet Service 2008; Kasim Sodangi (2021) What Nigeria Needs to Ask from Twitter, Techcabal (27 July 2021). Available at: https://techcabal.com/2021/07/27/what-nigeria-needs-to-ask-from-twitter.

160 Guidelines for the Provision of Internet Service.

161 Twitter operates as an intermediary.

162 Tage Kene-Okafor (2021) Twitter Ban in Nigeria to be Lifted if Platform Sets up a Local Office and Pays Taxes, President Says, TechCrunch (1 October 2021). Available at: https://techcrunch.com/2021/10/01/twitter-ban-in-nigeria-to-be-lifted-if-platform-sets-up-a-local-office-and-pay-taxes-president-says.

163 Nan (2021) Why Twitter, other platforms must register to operate, *The Guardian.* (11 June 2021). Available at: https://guardian.ng/news/why-twitter-other-platforms-must-register-to-operate-fg.

164 While yet to be enacted, the Intellectual Property Bill 2020 intends to simplify IP procedures by (among other things), incorporating all the current governing legislation – such as the Industrial Property Act 2001, Trade Marks Act (Revised 2012), Copyright Act 2001, and Anti-Counterfeit Act 2008 – into one Act.

165 Kenya Intellectual Property Bill 2020 s 238.

166 Kenya Computer Misuse and Cybercrimes Act 2018 ss 22–24, 27, 28, 37.

167 *The Bloggers Association of Kenya (BAKE) v Attorney General & 5 others* [2018] High Court of Kenya Petition 206.

168 Article 3(2) of the Law on Electronic Transactions defines intermediaries as "persons whose activity is to provide the public access to services through information and communication technologies".

169 Loi no. 2008-08 sur Les Transactions Electroniques s 3(2).

170 Ibid.

171 Ibid.

172 Tomslin Samme-Nlar (2018) *Why it is Important for African States to Ratify the Malabo Convention*, blog, African Academic Network on Internet Policy (31 July 2018). Available at: https://aanoip.org/why-it-is-important-for-african-states-to-ratify-the-malabo-convention.

173 WTO (2016) WTO Secretariat, General Council – *Fiscal Implications of the Customs Moratorium on Electronic Transmissions: The Case of Digitisable Goods*, WTO, JOB/GC/114.

174 Delegation of the European Union (2019) *Joint Statement on Electronic Commerce: EU Proposal for WTO Disciplines and Commitments Relating to Electronic Commerce*. INF/ECOM/22 3. Available at: https://trade.ec.europa.eu/doclib/docs/2019/may/tradoc_157880.pdf.

175 WTO (2017) Delegation of Indonesia, *Statement by Indonesia: Facilitator's Consultation on Electronic Commerce, MC11 Declaration, and Other Relevant Plenary Sessions* (13 December 2017). Available at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/68.pdf&Open=True; Nicolas Kohler-Suzuki (2020), *New Evidence on the Impact of Customs Duties for Digitisable Products and Electronic Transmissions: The Cases of Egypt and Vietnam*, Dalberg, 4. Available at: https://www.researchgate.net/publication/346787138_New_evidence_on_the_impact_of_customs_duties_for_digitizable_products_and_electronic_transmissions_The_cases_of_Egypt_and_Vietnam.

176 Law Insider, Carrier Medium Definition. Available at: https://www.lawinsider.com/dictionary/carrier-medium.

177 Delegation of the European Union (n 174).

178 WTO (2018) Delegations of South Africa and India, *Work Programme on Electronic Commerce – Moratorium on Customs Duties on Electronic Transmissions: Need for a Re-Think*, WT/GC/W/747. Available at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/GC/W747.pdf&Open=True.

179 WTO (2017) African Group, *The Work Programme on Electronic Commerce: Statement by the African Group*. Available at: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=239609,239579,239541,239472,239464,239336,239275,239266,239269,239278&CurrentCatalogueIdIndex=0&FullTextHash=&HasEnglishRecord=True&HasFrenchRecord=False&HasSpanishRecord=False.

180 Rashmi Banga (2019) *Growing Trade in Electronic Transmissions: Implications for the South*, UNCTAD. Available at: https://unctad.org/system/files/official-document/ser-rp-2019d1_en.pdf.

181 Simon Evenett (2021) *Is the WTO Moratorium on Customs Duties on E-Commerce Depriving Developing Countries of Much Needed Revenue?* St. Gallen Endowment, 5. Available at: https://currentthoughtsontrade.com/wp-content/uploads/2021/11/S.-Evenett_-WTO-Moratorium-12-Nov-2021_-finalised.pdf.

182 WTO (2020) Delegations of India and South Africa, *Work Programme on Electronic Commerce –The E-commerce Moratorium: Scope and Impact, Communication from India and South Africa*, 10 March 2020, https://commerce.gov.in/wp-content/uploads/2020/11/E-Commerce-Moratorium-Scope-and-Impact.pdf

183 WTO (2019) Delegations of India and South Africa, *Work Programme on Electronic Commerce – The E-Commerce Moratorium and Implications for Developing Countries: Communication from India and South Africa*. Available at: https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=254770,254764,254708,254719,254575,254574,254577,254349,254248,254192&CurrentCatalogueIdIndex=2&FullTextHash=237161575&HasEnglishRecord=True&HasFrenchRecord=True&HasSpanishRecord=True.

184 Centre for Intellectual Property and Information Technology Law (2021) *The Impact of the Proposed US-KE FTA on Kenya's Data and Digital Trade Policy*.

185 African Group WTO (n 179).


United Nations
Economic Commission for Africa


Digital
Pathways
at Oxford


BLAVATNIK
SCHOOL OF
GOVERNMENT
UNIVERSITY OF
OXFORD