ADDIS ABABA UNIVERSITY

COLLEGE OF LAW AND GOVERNANCE STUDIES

LL.M PROGRAM (BUSINESS LAW)

THE ROLE OF DATA LOCALIZATION LAWS OF ETHIOPIA IN REALIZING DIGITALIZATION TARGETS OF DIGITAL ETHIOPIA AGENDA 2025: COMPARATIVE STUDY

BY

BETHELHEM GEBRE

ID. NO.: GSE/9765/13

A THESIS SUBMITTED TO THE COLLEGE OF LAW AND GOVERNANCE STUDIES OF ADDIS ABABA UNIVERSITY IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE DEGREE OF MASTERS IN BUSINESS LAW (LLM)

ADVISOR: **DR. MANDEFRO ESHETE**

December 2024

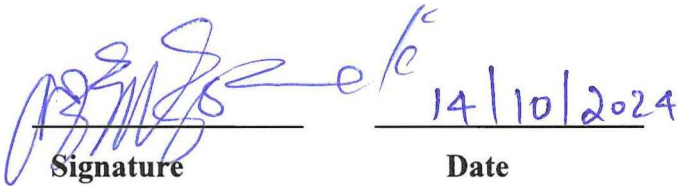
ADDIS ABABA UNIVERSITY

COLLEGE OF LAW AND GOVERNANCE STUDIES

BUSINESS LAW/ MASTER OF LAWS (LL.M) PROGRAM

THE ROLE OF DATA LOCALIZATION LAWS OF ETHIOPIA IN REALIZING DIGITALIZATION TARGETS OF DIGITAL ETHIOPIA AGENDA 2025: COMPARATIVE STUDY

Approved by:

Dr. Mandefro Eshete		
Advisor	**Signature**	**Date**
Dr. Biruk Haile	_____	_____
Examiner 1	**Signature**	**Date**
Dr. Jetu Edossa	_____	_____
Examiner 2	**Signature**	**Date**

DECLARATION

I, Bethelhem Gebre hereby declare that the work contained in this thesis is the result of a work I have carried out and whatever resources I have referred to have been acknowledged, and the relevant citations given.

…….

BETHELHEM GEBRE STUDENT

Submitted with Consent and Approval of:

……

DR. MANDEFRO ESHETE ADVISOR

DEDICATION

To my mother, Genet, you are my source of endurance and purpose in life- this work is for you.

ACKNOWLEDGMENT

I would like to express my deepest gratitude to my advisor, Dr. Mandefro Eshete, for his invaluable guidance, support, and patience throughout this journey.

I also want to extend my sincere thanks to Addis Ababa University School of Law for providing me with the resources and a conducive environment to pursue my research. The knowledge and experiences I have gained here have been integral to my academic and personal growth.

Lastly, I would like to thank my employer for their understanding and support during this time. Your flexibility and encouragement allowed me to balance my work and academic responsibilities, making this accomplishment possible.

Thank you.

LIST OF ABBREVIATIONS AND SYMBOLS

AfCFTA	**African Continental Free Trade Area**
AU	**African Union**
AU DTS	**African Union Digital Transformation Strategy**
AI	**Artificial Intelligence**
DDG	**Deputy Director General**
DTS	**Digital Transformation Strategy**
EU	**European Union**
ECA or Authority	**Ethiopian Communications Authority**
FDRE	**Federal Democratic Republic of Ethiopia**
GDPR	**General Data Protection Regulation**
GATS	**General Agreement on Trade in Services**
HPR	**House of People's Representative**
IT	**Information Technology**
ICT	**Information Communications Technology**
IOT	**Internet of Things**
NPDR	**Non-Personal Data Regulation**
OTT	**Over the TOP**

WTO	**World Trade Organization**

TABLE OF CONTENTS

Contents

Abstract

Policy documents such as the one this research will examine, i.e. Digital Ethiopia Agenda 2025, are a token to the desire of the Government of Ethiopia to building a digital eco-system and catching up with the rest of the world that had embarked on the digitalization journey long ago.

Digitalization is not just a matter of catching up with global fashion, the opportunities it brings with it are believed to be invaluable to small economies such as ours wishing to venture into global trade.

Building a digital economy, however, can be equated to placing structural bricks one by one as the eco system is composed of inter-complementary components. One of these components is the need to protect actors of the digital economy from potential abuse of their personal data. The brick of data protection framework, encompassing data protection laws and DPAs, is there to provide assurance that the digital space is a safe space.

Another one of such bricks is the need to enhance digital trade. If digital could not support economies such as ours by improving the cost and convenience of trade, arguably we have lost the use case for going digital.

These and other bricks forming the digital ecosystem must be well balanced to cause no harm and detriment on one another. That is; Digital trade must not flourish at the risk and compromise of digital safety and digital safety should not be too broadened where denial of approvals is perceived to be the only safety precaution.

A key area of interest is the free flow of data across jurisdictions; arguably, restrictions on the free flow of data limit a country's opportunity of fully benefiting from digital transformation and Privacy can be used as a pretext for imposing disguised restrictions on digital trade.

While Ethiopia may be a digital late starter, this is not a foreign concept to our jurisdiction. Utilizing the opportunity presented by the enactment of a comprehensive Personal Data Protection Proclamation in 2024, this research examined the conditions for cross border transfer of data set out under the Proclamation from the angle of achieving the digital transformation targets under the 2025 strategy document. The aim is to clear the ambiguity of the Country's position about data

localization and do a compatibility test with international and regional benchmarks. A comparative research method is utilized to analyze and interpret the findings of the research.

The research found out that via its data sovereignty principle, the Proclamation is set with strict data localization requirements where offshore processing and storage of data is prohibited for specified data sets. The research further found out that this sets Ethiopia apart from cited jurisdictions where predominantly conditional cross border data transfer is adopted as the best practice. Be that as it may, it is further found that localizing African's data in continental servers/ Data Centers is a recommended practice in the continental Digital transformation strategy document. However, the research's finding show incompatibility of the Proclamation with the four criterions of the AfCFTA's digital trade protocol which served as a test for legitimate restriction of free flow of data.

Key Words:

Data localization, digital transformation, data processing, cross border data transfer, data sovereignty

CHAPTER ONE: INTRODUCTION

1.1. Background and Problem Statement

'*The future of trade is digital and green…*'[1]

Restrictions to free flow of goods and services in form of traditional tariffs and non-tariff barriers is no longer a primary concern to the global economic community. Discussions around free trade are not perceived to be complete unless they address concerns about the free flow of Data. Data is the 'oil of the digital economy'[2], a nonrivalry form of oil that is neither depilated nor diminished through constant use.[3] with the Internet establishing itself as a preferred platform for economic and social activities, Data is not just a vehicle for economic transactions but also a factor of production used in the development of new products and services.[4]

From 2005-2022, according to WTO's digital trade estimate, digital trade of services has outpaced trade in goods and other services by an average annual increase of 8.1%.[5] The demand for Data consumption is constantly increasing with 463 exabytes of data estimated to be generated each day by 2025.[6] Every day incomprehensible amounts of data are created and stored across the internet.[7] In the past two years alone 90% of the world's data is generated with 250 million emails sent every

[1] < https://etradeforall.org/news/new-wto-world-bank-project-seeks-to-boost-africas-participation-in-digital-trade/> accessed 12 June 2024

[2] International Telecommunication Union and The World Bank, 'Data Protection and Trust' in Colin Blackman (ed), *Digital Regulation Handbook* (ITU Publications 2020)

[3] Yan Carrière-Swallow and Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective* (International Monetary Fund 2019)

[4] ibid 15.

[5] The World Bank and The World Trade Organization, *Turning Digital Trade into a Catalyst for African Development* (The World Bank Group 2023)

[6] Information Technology and Global Governance, *Data Governance and Policy in Africa* (Bitange Ndemo and others (eds) Springer Nature 2023) 30.

[7]< https://explodingtopics.com/blog/data-generated-per-day> accessed 15 August 2024

minute in 2022. [8] Those are constituted of various activities including online marketplace, messaging, cloud, and other social media activities.

With proliferation of data consumption, governance, and regulatory concerns arise. As much as data is treated as the 'oil' of digital economy, it's also characterized as a source of 'surveillance capitalism'[9], a source of strategic commercial assets. The need to adopt data protection[10] framework is self-evident today more than ever. However, the type of data protection framework created by policymakers will have a direct and long-lasting effect on how governments and citizens interact with digital ecosystems.[11]

The digital ecosystem is composed of inter-complementary components and data protection is but one component building the ecosystem. Another such component is the demand for Digital transformation in Africa. Digital Trade, a component of Digital transformation is a 'new source of growth and transformation in Africa'[12]. The cost and convenience of transacting goods and services is easier with digital technologies. These technologies afford African Countries a new 'Comparative advantage'[13] by providing them with a tool to overcome traditional trade barriers.[14] With improved digital connectivity and reduced costs of trade, Africa's share in the global export trade is expected to increase.[15] Through digital platforms, cross-border trade can be made on a more diversified portfolio of products including business services such as IT, and accounting.[16]

Emphasizing the critical role digital transformation brings for innovative, sustainable, and inclusive growth, the Digital transformation strategy for Africa 2020-2030("**AU DTS"**), makes

---

[8] ibid

[9] International Telecommunication Union and The World Bank (n 2) 99.

[10]Information Technology and Global Governance (n 6) 88. Note the difference between data governance and data protection, the later focuses on providing security to privacy, availability and integrity of data creation and utilization. Whereas the former focuses on rights and accountability for information related process.

[11] Michael Pisa and others, *Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity* (CGD Note 2021)

[12] The World Bank and The World Trade Organization (n 5)

[13] ibid

[14] ibid

[15] ibid

[16] ibid

'digitally enabled socio-economic development a high priority' in Africa. [17] 'Building digitally enabled pathways for inclusive prosperity' is a shared objective under the Digital Ethiopia 2025 strategy document.[18] In pursuit of this agenda, the AfCFTA Protocol on Digital Trade sets as its objective 'establishing harmonized rules and common principles and standards that enable and support digital trade…'[19]

There is an undeniable correlation between data protection and digital transformation. A digital ecosystem built on effective data protection laws translates to a greater reception of digital services by consumers.[20] Consumers are encouraged to use digital tools that rely on data sharing when they know that there is protection against misuse of their personal data. At the same time, digital transformation can flourish where there is an enabling regulatory environment.[21] A regulatory environment is perceived to be enabling when it 'promotes digital transactions while fostering trust in digital markets'.[22] The level of support data protection laws must provide to digital trade may be impaired by laws that impose an 'unreasonable burden on businesses'.[23] Contrary to the expected gain out of digital transitions, restrictive data protection laws hinder the setup and operation of organizations by increasing their burden and costs of production process.[24] A typical example of a restrictive data protection law is a prescriptive law that imposes data localization requirements and restricts cross border flow of data unreasonably.[25] Data localization requirements are criticized for diminishing organizations' efficiency by increasing the cost of doing business.[26]

---

[17] The Digital Transformation Strategy for Africa 2020-2030 (African Union)

[18]Digital Ethiopia 2025: A Digital Strategy for Ethiopia Inclusive Prosperity (The Federal Democratic Republic of Ethiopia)

[19] Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade (Durban Feb. 2024) STC-JLA [2024]

[20] Michael Pisa and others (n 11)

[21] The World Bank and The World Trade Organization (n 5)

[22] ibid 27.

[23] UNCTAD, *Data Protection Regulations, and International Data Flows: Implications for Trade and Development* (United Nations 2016) 19.

[24] ibid

[25] ibid

[26] ibid

The benefits of data protection laws are multifold. It's a highly preached theory with several scholarly writings building on the right of all humans to privacy. While that is not a subject of contest, it is equally important to examine the roles of data protection laws particularly laws that impose data localization requirements in building a digital economy and bringing digital transformation.

While this research is built upon previous studies made on cross-border data transfer requirements regionally and as part of multilateral trade regimes, to the best of the writer's knowledge no research is made to examine the position of the newly promulgated Personal Data Protection Proclamation No. 1321/2024 in regulating cross border data flow vis a vis its relationship with the sector-specific data protection requirement under Article 16(6) of the Telecommunications Consumer Rights and Protection Directive No. 832/2021 of Ethiopia. All to be seen from the perspective of building Digital Ethiopia 2025.

1.2. Review of Literature

To the best knowledge of the researcher, there is no domestically written literature addressing the subject matter of this research. Related domestic literature made on Ethiopia's digital transformation journey are reviewed in the absence of a domestic literature examining the policy rationale behind allowing or restricting cross border transfer of data. The gap in domestic literature is complemented by citing relevant writings of international organizations and authors.

In a contributory article by Tsegay Gebrekidan Telkeselassie captioned "Developing Ethiopia's Digital Economy: Lessons from China",[27] the article discusses the significant role that Ethiopia's digital policies and strategies play in shaping the country's digital economy. The article further emphasized that Information and Communication Technology (ICT) serves as an 'enabling tool' for developing a robust digital economy. The article's assessment highlights that the national development plans adopted by the Ethiopian government over the years have consistently incorporated components focused on ICT development.[28] From 2002 to 2010, national policy documents outlined specific ICT goals, emphasizing the importance of developing ICT not only as a standalone sector but also as a facilitator for other sectors of the economy. Despite these

[27] Tsegay Gebrekidan Tekleselassie, '*Developing Ethiopia's Digital Economy: Lessons from China'* [2021] ECIDC, Project Pape < Developing Ethiopia's Digital Economy: Lessons from China (unctad.org)> accessed 11 October 2024

[28] ibid

intentions, the article presents arguments that the government's monopoly over telecommunications, combined with inadequate ICT infrastructure, limited ICT skills, and affordability issues, has led to fragmented implementation efforts.[29] As a result, these challenges have hindered the country's progress toward establishing a comprehensive digital economy. The article points out that recent policy initiatives, introduced since 2020, aim to address the ICT challenges faced in previous years.[30] These initiatives include encouraging private sector participation in ICT development, building a national data center, and establishing capacity for big data analytics. He asserts that these strategies are better aligned with the goal of creating a vibrant digital economy in Ethiopia.

Investing in digital connectivity infrastructure on its own is not a guarantee for digital transformation.[31]A policy note jointly made by the World Bank and the World Trade Organization, indicates that countries can only reap the benefits of digital transformation if they intentionally put forth a conducive ecosystem for it to flourish.[32] The note also recognizes Data regulation to be at the 'heart of digital trade governance'[33]. Particularly with cross-border data flows, the policy note encourage policy makers to promote the 'sharing and transfer of data in a manner that supports the economic benefits of digital trade…'[34] In a study conducted by the World Bank, out of 26 sample countries in Africa, in half of them free flow of data is practiced incidentally due to a lack of regulation controlling cross-border data flows and not as a result of intentional choice made by policymakers. While there are countries that put forth requirements of keeping a copy of personal data in data centers within the host country's jurisdiction, that is criticized as it burdens trade and productivity of local companies using digital technologies.[35]

The cross-border nature of the Internet value chain highlights the need for cross-border collaboration and harmonization of regulations to aid the digitalization of economies.[36] It however

[29] Tsegay Gebrekidan Tekleselassie (n 27)
[30] ibid
[31] The World Bank and The World Trade Organization (n 5)
[32] ibid
[33] ibid 19.
[34] ibid 27.
[35] ibid
[36] International Telecommunication Union and The World Bank (n 2) 160.

is highly likely for consumers to develop 'risk-averse' [37]behaviors when they feel that their privacy right is not protected. Instead of increasing the uptake of digital services, the lack of a data protection regime could cripple the digital economy by influencing consumers' choices.[38] Recognizing the pivotal role personal data protection to the processing and free movement of such data, the 1995 Data Protection Directive of the European Union was adopted outlining guiding principles .[39] The Directive was later replaced by the General Data Protection Regulation (GDPR) in 2018.[40] These international and regional data protection regimes are set to avoid being 'too prescriptive' and maintain 'technology neutrality' so they don't become obsolete or hinder innovation.[41]

In explaining why countries are interested in regulating cross-borer data flow, a handbook prepared by ITU on digital regulation states the fear that organizations could use cross-border data transfer as a vehicle to forum shop and erode strong national data protections by transferring the data to a jurisdiction where there is no equitable personal data protection.[42]

Proponents of restriction substantiate their argument by citing the exceptions under the WTO GATS. Even where member states elect to liberalize their service sector they can apply exceptions to their obligations as per Article XIV (c) (ii) of the GTAS which states the ' Protection of privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individuals as a legitimate ground for applying the exception. As much as cross-border data transfer relates to transnational trade, trade rules allow exceptions necessary for safeguarding individual's privacy right.[43] On the contrary, opponents of the restriction argue that prohibition to cross border data transfer or data localization requirements can be used by states as disguised form of non-tariff barriers to trade.[44]

---

[37] ibid 152.

[38] ibid

[39] ibid 100.

[40] ibid

[41] ibid 103.

[42] ibid 124.

[43] ibid 106.

[44] International Telecommunication Union and The World Bank (n 2) 106.

A study conducted by the Center for Global Development identified three categories where data protection rules may be susceptible to poor design and enforcement. 'under-regulation', 'over-regulation', and 'regulating the wrong things in the wrong way'.[45] 'Under regulation' is when the impact of data protection laws is not visible in the real world. 'Over-regulation' occurs when compliance with data protection laws bears a high-cost impairing innovation. 'Regulating the wrong things in the wrong way' occurs due to overemphasis placed by most data protection laws on protecting against individual harm and not on collective harm.[46]

1.3 Research Question

This research is prepared with a central question of examining the role cross-border data transfer controls under the Ethiopian Personal Data Protection Proclamation No. 1321/2024 and the sector-specific data protection requirement of Telecommunications Consumer Rights and Protection Directive No. 832/2021 play in achieving the digital transformation agenda of Digital Ethiopia 2025.

In an effort to examine the central research question. The research will answer the following sub-questions.

1. Does the Ethiopian personal data protection law impose data localization requirements?
2. Is there conflict between the application of Personal Data Protection Proclamation No. 1321/2024 and sector specific data protection requirement found under Article 16(6) of Telecommunications Consumer Rights and Protection Directive No. 832/2021?
3. Does the requirement for cross-border transfer of personal data under the Ethiopian Personal Data Protection Proclamation pass the compatibility test with international/ regional best practices?

1.4.Research Objective

The primary objective of this research is to show the interplay between data protection laws and digital transformation. This research is not made to reinvent the wheel. It builds upon previous

[45] Michael Pisa and others (n 11)

[46] ibid 3.

studies and policy recommendations examining the role of regional/ national data protection laws in continental or national digital trade and transformation objectives.

The passing of the newly promulgated comprehensive Personal Data Protection Proclamation provides an opportunity to examine its role in realizing the digital transformation objectives of the country. The aim is to contribute to existing knowledge, understand the objectives of setting conditions for cross-border transfer of personal data, and examine if the conditions set forth miss or achieve the broader objective of digital transformation.

1.5.Research Method

1.5.1. Data

Data to carry out this research is obtained from the texts of Personal Data Protection Proclamation No. 1321/2024, Communications Service Proclamation No. 1148/2019, Telecommunications Consumer Rights and Protection Directive No. 832/2021, Telecommunications Quality of Service Directive No. 794/2021, SIM Cards Registration Directive No. 799/2021, Digital Ethiopia 2025, Convention on Cyber Security and Personal Data Protection (Malabo Convention), EU General Data Protection Regulation (GDPR), AfCFTA Protocol on Digital Trade, and the Africa Union Digital Transformation Strategy for Africa (2020–2030).

Texts about these laws are gathered from Scholarly writings, Parliamentary explanation notes, commentaries, discussion papers, and interviews.

1.5.2. Analysis & Interpretation

This research is made to assess the interplay between the digital transformation objective found under Digital Ethiopia 2025 and the law governing the protection and transfer of personal data. Assessments and interpretations of findings in this research are carried out using the thematic analysis (comparative analysis) and contextual interpretation techniques. This technique is best suited to answer for the research questions, as the aim of the research is to comparatively Alyse the Ethiopian Personal Data Protection Proclamation by conducting compatibility test with continental and global documents discussing data transfer and protection.

1.6.Limitation of the Study

The lack of domestic literature on this research topic has limited the study, necessitating a reliance on international writings to draw relevant lessons. Additionally, the adoption of the Personal Data Protection Proclamation just a few weeks before completing this thesis has created limitations, as the impact of the law on the industry could not be assessed due to its pending implementation. Furthermore, the regulatory body has yet to restructure its organization to accommodate supervision of Personal Data Protection, which has constrained the range of interviewees available for this study.

1.7. Thesis Organization

The thesis consists of five Chapters. The first Chapter covers introductory matters, including the background of the study, the statement of the problem, research questions, literature review, objectives, and methodology. The second Chapter provides a general understanding of the concept of digital transformation, with a focus on the AU Digital Transformation Strategy (DTS) and the Digital Ethiopia Agenda 2025. Chapter three defines cross-border data flow, outlines the scope of data under consideration, and discusses the rationale for regulating cross-border data transfer. Chapter four is dedicated to analyzing cross-border data transfer, examining common regulatory approaches by benchmarking the EU GDPR and the AfCFTA Digital Trade Protocol. It also analyzes Ethiopia's data localization requirements and concludes with a compatibility test against benchmark practices. Finally, Chapter five presents the findings and offers recommendations based on the research outcomes.

1.8.Referencing Rule

Ideas, expressions, and works of other researchers referred to in this research are cited using the rules of the Oxford University standard for the citation of legal authorities (OSCOLA 4th Edition).

CHAPTER TWO: DIGITAL TRANSFORMATION

2.1. Concept

Of relevance to this research is the concept of 'Digital Transformation'. Digital Transformation is among the competing policy rationales governments wish to strike a successful balance when setting up their data protection framework.[47]

Digital transformation is the process of 'integrating digital technologies into everyday life'.[48] It involves 'digitization'[49], a process of converting information from analog to digital format, and 'Digitalization'[50]a subsequent process of taking advantage of the digitization process by introducing increased efficiency and productivity.

Put simply, Digital Transformation dictates how societies and the economy can fully unleash the benefits of data.[51] This era of a data-driven socio-economic model has given rise to the 'Fourth Industrial Revolution'.[52] The emergence of evolving technologies such as blockchain, AI, Big Data analytics, and IoT is used by companies to devise a data-driven way of understanding behaviors for designing new products and services based on what the machine has learned to be fit to customer's needs.[53]

The transformation is expected to take place when Digital Technologies are used by various segments of the economy and society.[54] Its arm extends to government services, environmental management, agriculture, healthcare, education, and trade.[55] While this research is not intended to

[47] African Union Data Policy Framework (AU 2022)

[48] Information Technology and Global Governance (n 6) 133.

[49] ibid

[50] ibid

[51] AU Data Policy Framework (n 44)

[52] Alberto Lemma and others, *The AfCFTA: Unlocking the Potential of the Digital Economy in Africa* (ODI report 2022)

[53] ibid

[54] International Telecommunication Union, 'Good Regulation Broadens Access and Ignites Markets' in K. Stimpson (ed), *Global ICT Regulatory Outlook 2020: Pointing the Way Forward to Collaborative Regulation* (3rd edn, ITU Publications 2020)

[55] ibid

provide a deep dive analysis of Digital Transformation it is worth mentioning the definition proposed by a researcher in Montreal after having combined common properties of the concept.

'Digital Transformation is a process that aims to improve an entity by triggering a significant change to its properties through combinations of information, computing, communication, and connectivity technologies.'[56]

Four common properties are noticed in this definition. First, the entity targeted to take advantage of the transformation. Second, the degree of change within the target entity. Third, the technology used to bring transformation. And fourth, the desired outcome from the transformation.[57]

Having the above conceptual background, to the extent that digital transformation is influenced by data regulation; the research will briefly review the transformation goals of the continent as set under the AU DTS 2020-2030 and will go on to highlight the Digital Transformation goals under Digital Ethiopia 2025.

2.2. AU Digital Transformation Strategy for Africa 2020-2030

The DTS is a strategy document developed by the AU Commission in collaboration with multi-stakeholders. It identified six sectors that are critical to 'drive digital transformation'.[58] Those are Digital Industry, Digital Trade & Financial services, Digital Governance, Digital Education, Digital Health, and Digital Agriculture.[59] The strategy document is built up on Five foundation pillars and cross-cutting themes. Creating an enabling regulatory and policy environment is identified as the first foundation pillar, cyber security, privacy & personal data protection is among the cross-cutting themes considered in the DTS. The Commission has proposed recommended policies and actions for each component of the DTS. The research will concentrate on selected foundation pillars and cross-cutting themes relevant to the digital trade sector. This is in line with

[56] Vial G., *Understanding Digital Transformation: A Review and a Research Agenda* (The Journal of Strategic Information Systems 2019)

[57] ibid

[58] The Digital Transformation Strategy for Africa 2020-2030 (n 17)

[59] ibid

the objective of creating a 'digital single market'[60] through improved cross-border digital commerce and allow integration of the African data market through open standards.[61]

i. Enabling Environment, Policy & Regulation

As a component that sets a foundation for Digital Transformation, the DTS highlights the criticality of formulating an enabling regulatory and policy environment. For an enabling regulatory and policy environment to flourish, policymakers are advised to keep up-to-date with technological advancements, to support digital transformation through strategic documents, policies, and legislations, and governments to ensure the predictability and stability of the policy environment through political commitment.[62] The policy recommendation and proposed action highlight the need for creating a harmonized policy and legal and regulatory framework for achieving policy coherence among member states.[63]The DTS also suggests developing regulations that enable the free flow of non-personal data. [64] It further qualifies its recommendation by proposing local hosting of data necessary for e-services (within African countries) for reuse, exchange, and sharing in an open environment basis while adhering to data protection principles.[65]

ii. Cyber Security, Privacy and Personal Data Protection

Cybersecurity, Privacy, and Personal Data Protection are among the cross-cutting themes relevant to all the six digital sectors. Referring to the Malabo Convention and the increased volume of transborder personal data flow, the DTS recommends each nation adopt personal data protection strategies, a legal and regulatory environment.[66] It also encourages members to adopt a strong personal data legislation that gives improved control of personal data by its owners[67]. It further encourages nations to accelerate the formation of Personal Data Protection Authorities.[68] When it

[60] The Digital Transformation Strategy for Africa 2020-2030 (n 17)

[61] ibid

[62] ibid

[63] ibid

[64] ibid

[65] ibid

[66] ibid

[67] ibid 57.

[68] ibid

comes to data sharing and in particular with regards to the privacy of African citizens and residents, the DTS recommends adopting data localization law and supports ensuring commercial rights or a fair commercial share from the use of Africans personal data to stay in Africa[69].

2.3. Digital Ethiopia 2025. A Digital Strategy for Ethiopia Inclusive Prosperity

The Ethiopian Digital Transformation strategy is built on domestic and continental strategy documents including the 2019 Homegrown Economic Reform Agenda, the Ten-Year Development Plan, and the African Union's Continental Digital Strategy.[70] Priority sectors were selected based on the country's economic drivers and the national objective of creating jobs, forex earning, and inclusive prosperity.[71] Accordingly, Agriculture, manufacturing, mining, information and communications technologies (ICTs) enabled services, the creative industry and tourism are government priority sectors. [72]

The national strategy document highlights digital technologies' role in improving government services and increasing the country's competitiveness through e-commerce. A keynote is the government's desire to build a 'private sector led' economy where its role is to create an enabling environment based on a shift from a 'risk manager' to a 'development enabler' mindset that requires a 'trust-based' relationship with the private sector.[73]

Similar to the AU DTS, the national strategy document recognizes the importance of creating an enabling environment to complete the digital pathways. Various areas of improvement have been identified to enhance digital readiness. One of these areas is infrastructure.[74] This includes working to improve network coverage, affordability, and quality.[75] The strategy document acknowledges the telecom reforms that involve liberalizing the telecommunications sector as a good initiative but identified areas of improvement to accelerate telecom reforms through robust regulations.[76]

---

[69] The Digital Transformation Strategy for Africa 2020-2030 (n 17) 58.

[70] Digital Ethiopia 2025 (n 18)

[71] ibid

[72] ibid

[73] ibid

[74] ibid

[75] ibid

[76] ibid

The national strategy document highlights that Ethiopia is a 'late-starter' to digitalization initiatives and advises following a balanced approach that mitigates potential risks of digitalization.[77] One mitigation approach proposed by the strategy document is building the transformation goal on the existing development plans of the country.[78] Towards this end, the strategy document recognizes digital as an enabler of all other sectors, and regulating the ICT sector should follow a consultative and collaborative approach with a holistic view of the impact of digitalization on other sectors of the economy. Amongst enabling systems, the strategy document emphasizes the need to strengthen cyber awareness and security in the country and advises adopting 'cloud hosting and data centers.' [79]

[77] Digital Ethiopia 2025 (n 18)

[78] ibid

[79] ibid

CHAPTER THREE: UNDERSTANDING CROSS-BORDER DATA TRANSFER

It's established in the previous Chapter that the pathways leading to digital transformation must be built by enhanced digital readiness. Readiness can be achieved by adopting enabling policy and regulatory environment. An enabling environment maintains a delicate balance between the interest of promoting digital transactions on the one hand and the need to put restrictive measures to safeguard personal rights of individuals on the other.

This Chapter is prepared to discuss the second component of digital readiness, a component that is concerned with safeguarding the personal data of individuals. This component builds the digital economy, strengthening trust in digital transactions. However, this research will not go in-depth to legitimize the need for personal data protection laws, a topic sufficiently covered in many writings. A matter of interest to this Chapter is cross-border data flow, understanding what it is, its relationship with personal data protection, and its impact on the digital economy.

3.1. Defining Cross-Border Data Flow/ Data Localization Requirements

Cross-border data flow is concerned with the 'transfer of data to a foreign jurisdiction'.[80] It is also defined as 'the movement or transfer of data between servers across the borders of countries via networking equipment that enable such transmission".[81] A requirement that puts a limitation to the free flow of data is the 'data localization' requirement. This is a requirement limiting the processing and storage of data to a particular geographic area or jurisdiction[82], usually the data-originating jurisdiction.[83] The flow of data could also be limited to a group of countries, region, or

[80] UNCTAD (n 23) 28.

[81] Alexander Beyleveld and Franziska Sucker, *Cross-Border Data Flows in Africa: Policy Considerations for the AfCFTA Protocol on Digital Trade* (Mandela Institute 2022)

[82] European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European Data Economy"' COM (2017) 9 final

[83] Michael Pisa and others (n 11)

a province within a country.[84] There are many forms for imposing data localization requirements, broadly categorized as direct and indirect measures leading to data localization.[85]

Direct localization occurs when there is an express requirement for localization. This could be a law or a measure demanding copies of the data to be stored in local servers or restricting the transfer of data to outside jurisdictions.[86] Where the law/measure requires a copy of data to be stored in local servers, there is a possibility for transferring the data provided that there is a local copy. But in the latter category cross border data flow is not allowed even where copies of the data are kept in local servers.[87] Data localization could also materialize when the conditions put forth for transfer could not be met.[88]

The digital economy cares about the free flow of data partly because of data-driven services. These services, including computing, telecoms, media, finance, consultation, and others constitute 'half of the cross-border service trade'.[89] At times, it is unimaginable to have these services operationalize without some sort of data being shared across border. Border crossing of data may occur intentionally when a user is transferring a file to a non-resident abroad or unintentionally if data has to transit third party jurisdiction before reaching its user.[90] An email being sent between residents of the same country but the internet carrying the traffic routes through a third party jurisdiction or a user accessing OTT contents such as Facebook or Google but the content is stored in a server placed outside of the country are typical examples of unintentional border crossing of data by users. [91]

3.2.Scope of data under consideration in cross-border data flow

Cross-border data flow is usually concerned with the collection, use, and processing of data for generating data-driven insights into various domains of our lives. The data set in question may be

[84] Alexander Beyleveld and Franziska Sucker (n 77)

[85] ibid

[86] ibid

[87] ibid

[88] ibid

[89] Macmillan Keck and others, *The Role of Cross-Border Data Flows in the Digital Economy* (UNCDF 2022)

[90] ibid

[91] ibid

generated as byproducts of transactions but is used by evolving technologies such as AI, blockchain, and Big Data for improved decision-making. Evolving technologies require large and diversified data sets to generate insights to be used for innovating or improving processes, products, and decisions. [92]Online activities, click-through data, and buyer information are a few examples of data sets but not all of them are byproducts of direct human activity. A good example of data that is not a byproduct of human activity is machine-generated data. A communication made by the EU Commission on 'Building a European data economy' defines these types of data as 'created without the direct intervention of humans by a computer process, application or sensors'.[93] This leads to a discussion about the 'scope of data under consideration' when regulating cross-border data flow.

In principle, various types of data are capable of transmission across borders. However, policymakers do not intend to regulate all types of data sets. The distinction between personal and non-personal data demarcates policymakers' intention to intervene. The following summarizes the scope of selected legal/policy documents regulating cross-border data flow.

3.2.1. EU 2016/679 General Data Protection Regulation (GDPR)

Article 1(1) of the GDPR limits the scope of regulation to rules 'related to the protection of natural persons' concerning their 'personal data' including free movement and processing. Sub (3) further states that restriction on the free flow of 'personal data' is what the regulation intends to abolish. Non-personal data are outright excluded from GDPR's scope of regulation. Irrespective of its source, whether machine or human generated free flow of any personal data is within the ambit of GDPR's regulation.

3.2.2. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)

Defining the Convention's objective, Article 8 calls for state parties to commit to a stronger legal framework that involves punishing privacy violations without prejudice to the principle of free flow of 'personal data'. Article 9 further states that the Convention is concerned with 'any collection, processing, transmission, storage or use of personal data.'

[92] Macmillan Keck and others (n 86)

[93] European Commission (n 79)

3.2.3. Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade

Different from the Malabo convention, the scope of data under consideration for cross-border data transfer seems to go beyond personal data. Article 20(1) states, the annex on cross-border data transfer to be adopted after the Protocol, will govern matters to allow the transfer of data, including 'personal data'. While the annex on cross-border data transfer is under formation, the Protocol seems to envision governance of all types of data transfer.

3.2.4. Ethiopian Personal Data Protection Proclamation 1321/2024

The Proclamation's scope is limited to 'personal data'. Article 18 of the Proclamation which talks about the principles of data transfer states that its regulation is concerned with 'the transfer to a third party jurisdiction of 'personal data'. Article 20 sets conditions a data controller/processor must meet for the transfer of 'personal data'. Article 22 further states that data sovereignty applies to 'personal data' obtained locally.

3.3.What is 'Personal Data'?

The legislation/policy documents referred to adopt a similar definition to what amounts to 'personal data'. Three key elements can be gathered from these definitions. One, the data subject is a natural person. Two, the data is about an identified natural person and/or three, the data subject can be identified directly or indirectly by using a combination of identifiable information.

Table 1. Scope of data regulated in cross-border data transfer

	Scope	
	Personal Data	**Non-Personal Data**

GDPR[94]	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	
Malabo Convention[95]	any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly in particular reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identify	
AfCFTA Protocol on Digital Trade[96]	information and data, about identified or identifiable natural person by which such person can be identified, directly or indirectly	×
Personal Data Protection Proclamation 1321/2024[97]	any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the	

[94] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] L 119/1 Article 4(1)

[95] African Union Convention on Cyber Security and Personal Data Protection Adopted by the Twenty-Third Ordinary Session of the Assembly, Held in Malabo, Equatorial Guinea 27th June 2014 (Malabo Convention) [2014]

[96] AfCFTA Protocol on Digital Trade (n 19) art 1(q)

[97] Personal Data Protection Proclamation No. 1321/2024, art. 2(2)

	physical, physiological , genetic , mental , economic , cultural or social identity of that natural person;	

3.4.The Rational for Regulating Cross-Border Data Transfer

Various competing policy rationales influence government's decision to allow or restrict cross border flow of data. It's not surprising to know that privacy is not the only reason why governments wish to lock personal data within their jurisdiction. Yet, privacy laws that regulate cross-border transfer of personal data are concerned with 'surveillance capitalism'[98].To bring this concept home it's relevant to refer to applicable directives of the Ethiopian Communications Authority that dictate the type of information telecom operators are required to collect and retain when selling their products. The SIM Cards Registration Directive No. 799/2021 obliges Telecom Operators to collect minimum eight information from SIM card subscribers at the moment of subscription. Information such as full name, Nationality, date of Birth, gender, Physical address, postal Address, recent photograph, and biometrics accompanied by an identification document are required to be collected by Telecom Operators. [99] Similarly, Telecommunications Consumer Rights and Protection Directive No.6/2021 obliges Telecom Operators to keep their customers billing record for at least twelve (12) months. This Billing record includes:

A) [A] list of all calls made and services used, such as Value Added Services (VAS) made and/or used by the Consumer, and which includes number called, the date of the call, the start time, the duration and the price of the call indicating whether pricing is per minute, per second, per usage, or per capacity. b) An itemized list of the Consumer's national and international usage, monthly subscription fees, and premium rate charges. c) A list of data services used, including the date and time the session was initiated, the volume consumed in

[98]Alexander Beyleveld and Franziska Sucker (n 78)

[99] Telecommunications SIM Cards Registration Directive No. 799/2021, art. 8(1)

Mega Byte (MB), the duration of the session, the end date and time of the sessions and the price per MB. [100]

The data's are required to be retained by Telecom Operators even after the service is terminated.[101] Surveillance Capitalism goes beyond operator-collected data. Every day our smart devices track private information about our location, online activity and other private sensor information. Private information are freely used for prediction purposes and sold to companies commercially interested in knowing our activities to develop new products or send targeted ads.[102] Hence the growing skepticism around allowing cross border transfer of data.

Restrictions to cross border flow of data is also justified by non-privacy related policy rationales. Particularly with storing data outside of the country, governments fear that companies will not give access to local law enforcement authorities in need of the data for national security reasons.[103] They fear that data's stored outside of the country are exposed to surveillance by foreign governments.[104] Cyber security is another reason that informs government's decision to put restriction to cross border flow of data. There is a fear that by transferring the data to jurisdiction with weak cyber security framework, the data will be exposed to hacking and cyber-attacks.[105]

Most justifications put forth in support of cross border transfer are made based on certain economic rationale. Data localization requirements are criticized for being cumbersome that restrict businesses and slow them down from potential growth in the digital economy by exposing them to costly way of operation. The argument is, if companies operate in a restrictive data transfer environment, their chances of expansion in the cross-border economy, and growth based on data driven technologies will be stifled.[106] Digital trade is encouraged as it reduces the cost of transacting by removing traditional barriers to trade but if data transfer is restricted enterprises will be exposed to redundant investment, the cost of digital transactions will increase reducing

[100] Article 5 (4) Consumer Rights and Protection Directive No.6/2021

[101] Article 16(4) and 20(4) SIM Cards Registration Directive No. 799/2021

[102] Alexander Beyleveld and Franziska Sucker (n 78)

[103] Ibid

[104] Wickham Heath Consulting, *Cross-Border Data Flows Realizing Benefits and Removing Barriers* (GSMA 2018)

[105] ibid

[106] UNCTAD (n 23)

affordability to customers. Particularly with emerging technologies, unless free access of large, diversified data is facilitated and if data is kept in the jurisdiction of the originator to be processed separately, the socio- economic benefit we hope to drive from these technologies through digital insights and innovation will be restricted.[107]

But this too, has been criticized. Particularly in developing and least developed African countries, where there is 'digital inequality'[108] there has been questions on how cross border data transfer benefits Africans and small African digital platforms. This is mainly because most African countries are not in a position to benefit from the opportunities that cross border flow of data provides. Most of them including Ethiopia are 'digital latecomers'.[109] That means, they have big worries related to building digital readiness than facilitating the cross-border transfer of data such as expanding digital infrastructure, expanding their network coverage, increasing internet penetration, providing affordable internet services, providing affordable devices, covering the demand side gap including developing local contents and the list can go on. The question is, Africans remain net-data exporters.[110] The digital content that is being consumed in most African countries is content from outside of the continent. large scale Multinational digital platforms such as Facebook and Google are being compared with the non-existing African digital platforms. The assertion is, Africans are being requested to supply data to the rest of the world without taking any substantial benefit from it.[111] Proponents of this argument see nothing wrong with African countries demanding data localization aimed at developing the domestic digital infrastructure such as requesting multinationals to build local data centers to store local contents. This position is labeled as 'digital protectionism'[112] as some say it has trade distorting effects as the measure is intended at granting a competitive advantage to domestic actors engaged in digital trade from their foreign competitors.[113]

---

[107] European Commission (n 79)

[108] ibid

[109] Digital Ethiopia

[110] Alexander Beyleveld and Franziska Sucker (n 78)

[111] ibid

[112] Wickham Heath Consulting (n 101)

[113] Alexander Beyleveld and Franziska Sucker (n 78) 46.

CHAPTER FOUR: REGULATING CROSS BORDER DATA TRANSFER

The opportunities presented by the digital economy are multifold. However, building a digital economy is not free from challenges. The solutions adopted by governments to these challenges should not cripple digitalization nor erode superior policy rationales such as privacy and national security. As discussed in the previous Chapter, various economic and non-economic rationales have dictated how governments regulate data transfer to foreign jurisdictions. In this Chapter, common forms of regulating cross-border transfer of data will be discussed to make comparisons with the Ethiopian Personal Data Protection Proclamation and draw insights from well-known data regulating legislations/agreements.

4.1. Common Approaches of Regulating Cross-Border Data Transfer

In the absence of a single unified international data protection rule, different approaches are followed across jurisdictions to moderate how data transfer, if at all permitted can be made. A study held by the GSMA identified common approaches governments use for regulating cross-border data transfer.

4.1.1. Conditional Data transfer leading to de-facto data localization

In most jurisdictions, cross-border data transfer is permitted provided that the conditions put forth for the transfer are complied with. From requiring regulatory approval to obtaining consent from data subjects to demonstrating the adequacy of the data protection rules of the foreign jurisdiction various conditions are placed to restrict or allow the transfer of data across jurisdictions.

A common form of conditional data transfer is made by providing exceptional scenarios for a specific transfer. Certain exceptions to cross-border data transfer are common across jurisdictions and found in almost all legislations regulating cross-border data transfer.

Some of the broadly accepted exceptional scenarios include:

The transfer is necessary for the performance of a contract between the data subject and the controller or between the controller and a third party and (i) is entered into at the request of the data subject; or (ii) is in the interests of the data subject; The transfer is for the purpose of legal

proceedings or for the purpose of obtaining legal advice or for establishing, exercising or defending legal rights; or The transfer is necessary in order to protect the vital interests of the data subject.[114]

While they may not be broadly accepted as the exceptions discussed above, there are types of exceptions that are fragmentedly applied across jurisdictions.

i. **'whitelist' Approach**[115]:- Some countries follow an approach of assessing the level of adequacy of the third-party jurisdiction's data protection regime in protecting the personal data of the data subjects. Where it is found to be adequate, the entire third-party jurisdiction will get clearance for receiving transfer of personal data.
ii. **'Binding Rules'**[116] Particularly applicable within certain corporate groups, this modality assesses whether the companies within the group have sufficient data protection framework. Where the sufficiency of the data protection process is verified through independent assessment, the data will be allowed to freely move within the group of companies.
iii. **'Model Contract'** [117]Requires companies to agree on model contractual clauses that are drafted to provide a sufficient degree of protection for the transfer of personal data. Where companies are not willing to adopt the wording of the model contract, the transfer will not be permitted.
iv. '**Consent'**[118] This is where the transfer is conditional on getting the consent of the data subjects for the transfer of their personal data to a foreign jurisdiction. The type of consent required may vary across jurisdictions. This approach is criticized as consent is prone to various interpretations which may lead to disputes. Particularly where there is an imbalance in bargaining power between the contracting parties, data subjects may be coerced to provide their consent.

[114] UNCTAD (n 23) 28.

[115] ibid

[116] ibid

[117] ibid

[118] ibid

4.1.2. Data Localization

This is a requirement limiting the processing and storage of data to a particular geographic area or jurisdiction[119], usually the data-originating jurisdiction. This requirement of keeping data in its home country may be imposed directly or indirectly. It is imposed directly when there is an express requirement for localization.[120] Organizations may be required to store locally acquired data in local servers and data centers. Data localization could also happen through demanding local presence. This is a case where governments require offshore service providers to establish a permanent establishment or representative office locally and keep local data in local servers.[121] In some jurisdictions cross border transfer of data is outright prohibited particularly applicable to information known to be sensitive. [122]In this case, companies will not have an option but to store and process personal data locally. Even where there is no prohibition, the conditions set for allowing the transfer discussed in Section 4.1.1., maybe too stringent to comply with, strategically discouraging any form of transfer.[123]

4.2. EU 2016/679 General Data Protection Regulation (GDPR)

While the EU has a separate framework, EU NPDR, for regulating cross-border transfer of non-personal data, the GDPR is primarily concerned with protecting the 'fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data'[124] and hence its regulations on cross-border data transfer are targeted towards personal data.

The EU GDPR is the epitome of conditional cross-border data transfer. Chapter five of the GDPR sets out the conditions that need to be met for a transfer of personal data to third countries or international organizations. Article 44 of the GDRP states 'any transfer of personal data …shall take place only if, subject to other provisions of this Regulation, the conditions laid down in this Chapter are complied with.'[125]

---

[119] European Commission (n 79)

[120] Kholofelo Kugler, T*he Impact of Data Localisation Laws on Trade in Africa* (Mandela Institute 2022)

[121] Wickham Heath Consulting (n 101)

[122] ibid

[123] ibid

[124] Regulation (EU) 2016/679 (n 90) art 1(2)

[125] Regulation (EU) 2016/679 (n 91) art 44 (1)

i. 'Adequacy Approach'

Article 45 of the GDPR provides a condition where personal data can be transferred to a third country or international organization provided that the third country or international organization 'ensures an adequate level of protection.'[126] The GDPR whitelists these countries, or international organizations that pass the adequacy test without a need to acquire a specific authorization for the transfer. [127] The 'implementation act' that is granted to countries, specified sector or an international organization that passes the adequacy test is subject to a period review of at least every four years.[128] Where the adequate level of protection is found to not be upheld through the periodic review, the whitelist can be repealed, amended, or suspended.[129]The parameters used for testing the level of adequacy is found under Article 45 (2) a -c of the GDPR. The provision reads:

> [*T]he rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred*.[130]

Beyond assessing the rule of law in the third country jurisdiction, the adequacy test also examines the independence, enforcement power, and cooperativeness of the data protection supervisory authorities in these jurisdictions.[131] Any international, regional, or multilateral commitments related to protection of personal data made by the third country or international organization are

---

[126] ibid art 44(1)

[127] ibid art 45 (1)

[128] ibid art 45(3)

[129] ibid art 45(5)

[130] ibid art 45(2)a *emphasis added*

[131] ibid art 45(2) b

also assessed as part of the adequacy test.[132] The adequacy test of the GDPR is criticized for giving broad discretions to the Commission due to its long list of requirements which are perceived to be difficult to attain and in effect normalize data localization instead of transfer.[133]

ii. 'Appropriate Safeguards'

The GDPR provides for a condition where a transfer can be made possible in case a Data Controller or Processor provides appropriate safeguards to the rights of data subjects. [134] As provided under Article 46 (2) of the GDPR, the appropriateness of the safeguard mechanism can be demonstrated by making use of a legally binding instrument between public authorities, binding corporate rules, standard data protection clauses adopted by the commission or supervisory authority, or contractual clause by supervisory authority provided that the safeguards ensure compliance with data protection and the right to effective legal remedy in case of violation.[135] When safeguards are provided for in administrative arrangements that are not binding or a contractual clause between the data controller/processors of the two jurisdiction, for a transfer to be made possible authorization by the competent supervisory authority is required.[136]

iii. 'Binding Corporate Rule'

Applicable to a group of undertaking who wish to transfer data within the group by getting their corporate rule approved. The corporate rule in question should be legally binding, applied, and enforced across all enterprises within the group, include all essential principles, and provide enforceable rights to data subjects concerning the processing of their personal data.[137]

iv. 'Transfer Based on Extraterritorial Rules of Third Countries'

The GDPR under Article 48 boldly states that a transfer of data or disclosure will not be made based on any court/tribunal or decision of an administrative authority of a third country, unless the

[132] Regulation (EU) 2016/679 (n 91) art 45 (2) c

[133] Alexander Beyleveld and Franziska Sucker (n 78)

[134] Regulation (EU) 2016/679 (n 91) art 46 (1)

[135] ibid art 46(2) a-f

[136] ibid art 46(3)

[137] ibid art 47(1)

request is made as part of an international agreement or mutual legal assistance treaty between the two jurisdictions.[138]

v. Conditional Transfer

The GDPR provides exceptions where cross-border data transfer can be made under specific conditions. Those conditions include.

a. Where explicit consent is acquired from the data subject after having been informed of the risks of the transfer.[139]
b. Transfer is necessary for performance of contractual obligations or pre-contractual measures between the data subject and controller, or a contract concluded in the interest of the data subject between the controller and a third person.[140]
c. Transfer is necessary for reasons of public interest or the establishing exercise and defense of a legal claim.[141]
d. In case the data subject is not able to give his consent, a transfer could be allowed if necessary to protect the vital interests of the data subject.[142]
e. Where transfer is made from a register that is open for public or interested party consultation[143] the GDPR also permits a non-repetitive transfer that concerns a limited number of data subjects in residual cases such as historical, scientific, or historical purposes.[144]

The GDPR provides extensive grounds and conditions for transferring data across jurisdictions. Any restriction to cross-border transfer of data for failing to meet the conditions laid under the regulation is perceived to be legitimate restriction to cross-border data transfer. This has led to

[138] Regulation (EU) 2016/679 (n 91) art 48

[139] ibid art 49(1) a

[140] ibid art 49(1) b & c

[141] ibid art 49 (1) d & e

[142] ibid art 49 (1) f

[143] ibid art 49(1) g

[144] ibid art 49(1) para 2

criticisms that by setting unattainable conditions, the GDPR is placing a de-facto data localization regime.[145]

4.3. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)

When it comes to personal data protection, the Malabo Convention was clear in its objective that the protection should come from a domestic legal framework that state parties are required to establish. The national laws should safeguard protection and punish violations.[146] The Convention does not have specific rules or conditions that guide on cross-border transfer of personal data. Rather, Article 11 (1) of the Convention requires state parties to establish national authorities in charge of protecting personal data. The Convention provides that the national authorities should be responsible for authorizing the trans-border transfer of personal data.[147]

4.4. Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade

Unlike the Malabo Convention, the Protocol on Digital Trade governs the cross-border transfer of data by setting high-level principles and outlining a framework where the detailed rules will be specified in an annex on cross-border data transfer which is currently under formation. The general principle under the Protocol dictates, so long as the transfer is to conduct digital trade, state parties should permit transboundary transfer of data.[148] However, the Protocol sets a four-part test where restriction can be legitimately permitted.[149] Article 20(2) of the Protocol allows a restrictive measure where the measure:

i. Is applied to 'achieve legitimate public policy objective or protect essential security interests.'
ii. Must not be 'applied in a manner which would constitute a means of arbitrary or unjustified discrimination'.

[145] Policy consideration for the AFCFTA protocol on Digital trade

[146] Malabo Convention (n 92) art 8(1)

[147] Malabo Convention (n 92) art 12 (2) k

[148] AfCFTA Protocol on Digital Trade (n 19) art 20 (1)

[149] AfCFTA Protocol on Digital Trade (n 19) art 20 (2)

iii. Should not constitute a 'disguised restriction on digital trade'.

iv. 'Does not impose restriction on transfer of data greater than are required to achieve the objective.'

4.5. Ethiopian Personal Data Protection Proclamation 1321/2024

Speaking of its objective, the one-month-old Proclamation as of writing this research states the need to 'capitalize on beneficial opportunities presented by cross-border transfer of personal data both into and out of the country'.[150] The type of data the Proclamation is concerned about is data originating from Ethiopia and excludes any data originating from outside of the country or transiting through Ethiopia from a third country.[151] This is a Proclamation that applies across all sectors of 'private and public institutions'[152]throughout the country. It is however limited to Data Controller or Data Processor 'established in Ethiopia' and who does the processing in relation to the activity of the establishment.[153] If not established in Ethiopia, the Data Processor or Controller need to have a 'representative', and equipment placed in Ethiopia for processing.[154]

The principle for data transfer under Article 18 of the Proclamation states that a transfer to a third-party jurisdiction could take place if the third-party jurisdiction ensures 'appropriate levels of protection'.[155]

i. 'Appropriate Level of Protection' in Third Rarty Jurisdiction

The standards set under Article 19 of the Proclamation for measuring level of appropriateness of the third-party jurisdiction's personal data protection framework is equivalent to the GDPR's 'adequacy test'. Similar to Article 45(2) of the GDPR, the Proclamation lists matters that will be put in consideration for measuring 'appropriateness'. Article 19(2) of the Proclamation states:

> [*P]articular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of*

[150] Personal Data Protection Proclamation, (n 93) Preamble para. 4

[151] ibid art.3(4) d

[152] ibid art.3(3)

[153] ibid art.3(2)a

[154] ibid art. 3(2)b

[155] ibid art. 18

> *origin and country of final destination, the rules of law in force in the third-party jurisdiction, and the professional rules and security measures which are compiled within that jurisdiction*.[156]

Compared to GDPR, the areas that the Proclamation assesses for determining appropriateness appears to be narrower in scope. However, the appropriateness test under the Proclamation is subject to general jargon like demonstrating the existence of the rule of law in third-party jurisdiction including assessing the existence of professional rules and security measures. The Proclamation doesn't indicate the type of evidence the Authority will take into account for demonstrating the existence of the rule of law nor does it tell which professional rule and security measure it is intending to examine in the third-party jurisdiction. Article 5(10) of the Proclamation that gives mandate to the Authority states that the determination is made in comparison to the level of protection the Proclamation provides.[157] The Data Controller or Data Processor is required to provide evidence to the Authority to demonstrate the appropriate level of protection in the third-party jurisdiction based on which the Authority will make its determination.[158] On the type of evidence a Data Controller or Processor must provide for demonstrating appropriate level of protection, in an interview held with the Deputy Director General of the Ethiopian Communications Authority, the DDG explained, 'the type of evidences are listed in Article 19(2) of the Proclamation. The interest of the Authority is to demonstrate the legal and regulatory framework related to data protection and enforcement of these laws in the third-party jurisdiction.'[159] 'The Authority also requires security and operational level details of the recipient organization to be provided as part of evidence demonstrating the existence of appropriate level of protection.'[160] The Proclamation doesn't place an obligation on the Authority to provide reasons why a third-party jurisdiction doesn't acquire the appropriate decision and gives extensive discretion by placing the burden of proof on the Data Controller or Data Processor requesting the transfer.

---

[156] Personal Data Protection Proclamation (n 93) art.19(2) *emphasis added*

[157] ibid art. 5(10)

[158] ibid art. 20(1)a

[159] Interview with Million H/Michale, Ethiopian Communications Authority Deputy Director General, August 2024

[160] ibid

ii. 'Limited Form of Transfer in the Absence of Appropriateness'

A new approach introduced under the Proclamation not necessarily found under the GDPR is allowing a limited form of transfer in a manner that doesn't violate the data subject's right under the Proclamation.[161] This is applicable where the third-party jurisdiction could not acquire the appropriateness decision under Article 19(2) of the Proclamation. However, how limited is a limited transfer is not put under the Proclamation.

A limited form of transfer can be facilitated in case it fulfills two requirements. The data subject's consent for the transfer and reduction in aspects of the data which it deems appropriate.[162] Consent is defined in the Proclamation as 'freely given specific, informed and unambiguous indication of the wishes of the data subject' either made in writing, verbally, or through gesture.[163] Demonstrating the existence of consent could be contentious provided that the Proclamation accepts consent made verbally or through gesture. The DDG of the ECA also explained that ' the Authority recognizes that not all third party jurisdictions will meet the appropriateness test under Article 19 (2) of the Proclamation. A limited form of transfer is provided to support transactions that involve countries that have not met the appropriateness test. The role of the Authority will be authorizing the transfer as per Article 19(3) of the Proclamation and make necessary adjustments by reducing the data that will expose the data subject to risks.'[164]

iii. '**Conditional Data Transfer'**

Alongside the appropriateness decision obtained from the Authority, a few other conditions are put to allow the transfer of data to a third-party jurisdiction.

a) Consent

Acquiring the data subject's explicit consent for the transfer after notifying the potential risks is an accepted ground for transferring personal data across borders.[165] It is not clear how this is

[161] Ethiopian Personal Data Protection Proclamation (n 93) art. 9(3)

[162] ibid art.19(4) a &b

[163] ibid art. 2(14)

[164] Interview with Deputy Director General of the Ethiopian Communications Authority (n 156)

[165] ibid art. 20 (b)

different from the consent required for a limited form of transfer under Article 19(4) of the Proclamation.

b) Necessity Test

The Proclamation puts five conditions where a transfer is perceived to be necessary. Similar to GDPR, a transfer is necessary if used for performance of contractual obligations or pre-contractual measures between the data subject and Controller or a contract concluded in the interest of the data subject between the Controller and a third person. [166]A transfer is also believed to be necessary 'for reasons of public interest, establishment, exercise and defense of a legal claim or to protect the vital interest of the data subject or other persons in case the data subject is not able to give his consent for legal and physical reasons.'[167]

c) Public database

A transfer of personal data can be made effective if the data is obtained from a register that is kept to give information to the public.[168]

Conditional transfers except for a transfer made pursuant to the appropriateness test are not dependent on getting the Authority's pre-approval. However, the Authority is given the discretion to request the person doing the transfer 'demonstrate the effectiveness of its security safeguards and existence of compelling legitimate interest'.[169] The Authority's discretion extends to 'prohibiting, suspending or subjecting the transfer to such conditions that the Authority determines'.[170]

iv. Data Localization

The Proclamation boldly sets a strict data localization rule by requiring personal data collected or obtained locally to be stored in local servers or data centers.[171] This, according to the Proclamation

[166] ibid art. 20 (2) b

[167] ibid art. 20 (2) c-e

[168] ibid art. 20 (1) (d)

[169] ibid art. 21(1)

[170] ibid art. 21(2)

[171] ibid art. 22 (1)

is part of the 'data sovereignty' rule consideration of which may not be limited to safeguarding personal data of data subjects. It further gives a mandate to the Authority to prescribe categories of personal data that are **critical** and shall only be processed in local server or data center.[172] The criticality is determined based on 'strategic interest of the state'.[173] This might be one of the most controversial clauses of the Proclamation when it comes to regulating cross-border data flow. Generally, even where data is required to be stored locally, a copy of the data can be transferred across borders provided that the conditions for the transfer are met. However, for the category of data which the Authority is going to label as critical, there will not be any room for transferring the data as these are required to be processed locally. It is important to note that, the consideration here is not just privacy but other 'strategic interest of the state'. On what determines the criticality of personal data, the DDG explained 'factors beyond privacy including national security, public interest, and other security reasons will guide the Authority's determination'.[174]. the DDG further explained that ' the data sovereignty principle set under the Proclamation maintains a balance between data transfer needs (provided that the conditions for the transfer are met) and the need to retain data locally to allow economic benefit from data, national security, public and other strategic interest of the state.' [175]As this is a new Proclamation, the Authority has not yet prescribed critical personal data for which transfer is not allowed. Until the Authority prescribes critical categories of personal data, Data Controllers/ Processors may not fully exercise transfer rights based on necessity, consent, and public database grounds.

v. **Sensitive Personal Data**

Sensitive personal data as defined under Article 1(5) of the Proclamation[176] can only be transferred across jurisdictions provided that the Authority gives pre-approval for the

[172] ibid art. 22(2)

[173] ibid art. 22(2)

[174] Interview with Deputy Director General of the Ethiopian Communications Authority (n 156)

[175] ibid

[176] Ethiopian Personal Data Protection Proclamation (n 92) art. 1(5) Sensitive personal data are natural person data on a) Racial or ethnic origins; b) Genetic or biometric data; c) Physical or mental health or condition Political opinions; e) Membership of a professional association ; f) Religious beliefs or other opinion of a similar nature; g) The commission or alleged commission of an offence; h) Any proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in the proceedings; i) Communications

transfer.[177] The proclamation doesn't provide guidance on factors the Authority will take into account for allowing or restricting the transfer.

Irrespective of the conditions that warrant cross-border data transfer, Article 48(1) of the Proclamation imposes obligation on Data Controllers/Processors to obtain prior authorization from the Authority before transferring the data to third-party jurisdictions. This is justified as a necessary measure for safeguarding the rights of data subjects to avoid risks associated with the lack of providing appropriate safeguards for the transfer.

Similarly, Article 45(1) of the Proclamation requires a prior security check to be conducted by the Authority in case the Authority 'is of the opinion that the processing or transfer of data by a Data Controller or Data Processor may entail a specific risk to the privacy rights of data subjects".[178] A Data Controller/Processor is required to record 'any transfer of data to another country, and the suitable safeguards'.[179]

On whether there's a need to get the Authority's pre-approval for all data transfer requests, the DDG of the ECA explained 'the Proclamation doesn't envision getting the Authority's consent for all data transfer requests except for transfer based on appropriateness and limited form of transfer. However, the Authority does have the mandate to intervene incase its identified in the risk assessment that the Data Controller/ Processor did not deploy proper security measures to safeguard data subject's personal data.'[180]

4.5.1. Telecommunications Consumer Rights and Protection Directive No.6/2021

In cognizance of the vulnerabilities of telecommunications service consumers, the Ethiopian Communications Authority, mandated to safeguard the interest of consumers of telecommunications service had enacted the sector-specific Directive to govern and safeguard the

---

data, including content and metadata; or j) Any other personal data that the Authority may determine as sensitive personal data from time to time.

[177] ibid art. 22 (3)

[178] ibid art. 45 (1)

[179] ibid art. 46(2)e

[180] Interview with Deputy Director General of the Ethiopian Communications Authority (n 156)

personal data and rights of telecommunications service consumers in line with the stipulations of Article 6(14) of the Communications Service Proclamation No. 1148/2019.

Part six, Article 14 of the Directive sets out requirements where consumers privacy can be safeguarded. Amongst the safeguard measures is an obligation on telecommunications service providers to develop a policy for protecting consumers privacy. The policy is expected to outline the type, use and conditions for transfer and exchange of personal data including the choices available to consumers.[181] Particularly with regards to the transfer of consumer's personal data, the Directive doesn't allow a transfer unless there is explicit consent from the consumer.[182] It further states that any information on consumers is not allowed to be transferred to any party unless mandated by a court order or through explicit consent of the consumer made in writing or other verifiable means.[183] When it comes to data localization, the Directive boldly states that consumer's personal data shall only be processed in a server or data center located in Ethiopia.[184]

4.6. Personal Data Protection Proclamation and its relationship with the sector-specific consumer data protection rules

Data localization is not a new requirement introduced under the Personal Data Protection Proclamation, at least for telecommunications services, consumer's personal data has been required to be processed in local servers and data centers since the enactment of the Directive in 2019. The Directive does not hold a specific clause addressing the transfer of personal data across jurisdictions. The only plausible ground was a transfer based on explicit consent of data subjects. The focus of the Directive was mostly on disclosure of personal data to third parties for law enforcement purposes provided that a court order is produced. This however envisions local data transfer and does not apply to transfers made across borders. The lack of clarity has led over-compliant organizations to avoid utilizing services such as cloud hosting that are dependent on cross-border data transfer.

[181] Telecommunications Consumer Rights and Protection Directive No. 832/2021, art. 15 (2) & (3)

[182] ibid art. 15(3)

[183] ibid art. 16(5)

[184] ibid art. 16(6)

Compared to the Directive, the Data Protection Proclamation clears the ambiguity and provides more grounds for transferring data across jurisdictions. This doesn't mean that the Proclamation has abolished the data localization requirement outlined under the Directive. The data sovereignty rule under Article 22(1) of the Proclamation requires all personal data originating from Ethiopia to be stored in local servers and data centers. However, lessons from benchmark practices indicate that even where personal data is required to be stored locally, a copy of the data can be subsequently transferred provided that the preconditions set for the transfer are met. The Proclamation is more elaborate on the permissible grounds for cross-border data transfer. The Proclamation allows a transfer to be made based on 'Appropriate Level of Protection' in third party jurisdiction, a 'Limited Form of Transfer in the Absence of Appropriateness', 'Conditional Data Transfer based on consent, necessity or public database. Those are grounds that were not recognized under the Directive which completely blocks the processing of personal data in offshore servers and data centers, however, the Proclamation under Article 22 (2) restricts cross-border transfer to categories of data prescribed to be critical by the Authority for reasons accounting to 'strategic interest of the state'.

The Proclamation does not explicitly repeal the Directive nor is it placed in equal hierarchy of law with the Directive. In case there is any ambiguity on the applicability of part six of the Directive, Article 67 of the Proclamation clears that ambiguity by making any contradicting laws or customary practices non-applicable.

An interesting correlation between the two laws is that they are supervised by the same regulator body, The Ethiopian Communications Authority. The assessment of the powers given to the ECA indicates the interest of the Ethiopian government in moving towards a converged approach of regulation. The jurisdictional debate of how much power an ICT regulator should assume to answer for the modern-day challenges of digital transformation is settled by expanding the scope of mandates given to the telecom regulator. The contemporary issues that emanate from digital transformation such as competition, data protection, and cyber security are new issues that the ECA is mandated to oversee pursuant to the Communication Service and Data Protection Proclamation. The Communications Services Proclamation under Article 16 states the vision of the government to use the sector as a platform for economic and social development in the country.

It is also worth noting that the ECA is given the flexibility to set up its own administrative structure that it believes is appropriate to carry out personal data protection responsibilities.[185] However, it's also important to note that the ECA was first established in 2019 via the Communications Services Proclamation which makes it amongst the youngest regulatory bodies in Ethiopia. Accommodating both responsibilities that originate from the Communications Services Proclamation and the Personal Data Protection Proclamation requires the ECA to establish its institutional independence by way of building its capacity, creating a culture of independence, and upskilling its human resources. This includes granting the Authority full financial independence. As it stands pursuant to Article 17(1) a of the Communication Services Proclamation, the ECA is required to use a budget allocated to it by the government.

4.7. Insight into Current practice of a Service Provider

Businesses of all types can arguably benefit from a cross-border data flow scheme. This benefit is believed to be heightened when the business is multinational looking to enhance competitiveness by reducing cost and improving business efficiency.[186] With cross border data flow, multinational organizations will be able to centralize their internal operation through digitalization.[187] By leveraging cloud-based infrastructures, they can utilize a single supplier and specialized service provision for their nationwide operations, thereby improving the quality of their operation and reducing investment costs, which can ultimately enhance their competitiveness.[188]

Given the extent of personal data collected by telecom operators, the regulatory body, ECA has imposed sector specific privacy obligations applicable to all actors in the industry. The obligation extends to adopting a privacy policy and communicating customers of the type of personal data collected, the use, exchange including international transfer of that data and choices available to consumers[189]. The privacy policy of the first foreign private telecom operator, Safaricom Telecommunications Ethiopia plc speaks of the current practice that multinationals such as Safaricom Ethiopia opted to concerning the processing and transfer of personal data to third party

[185] Personal Data Protection Proclamation (n 93), art. 5(2)

[186] GSMA (n 102)

[187] ibid

[188] ibid

[189] Telecommunications Consumer Rights and Protection Directive (n 179), art. 15 (2)

jurisdictions. According to Safaricom Ethiopia's privacy statement published in its official website,[190] the operator may collect variety of information from its customers depending on the product/service the customer subscribed to, the use of the product/service and customer interactions with the service provider. Accordingly, Safaricom Ethiopia, as communicated in its privacy policy, may collect personal information: Includes name, address, phone numbers, date of birth, gender, and email. bank information, traffic data: Covering information on calls made, their duration, and data usage patterns. location data, correspondence with Safaricom, Account Information, credential information, preferences, information about user preferences for products and services, data sessions and service usage data, information on how users interact with products and services, including service quality and network issues, These information may further be processed, depending on the type of service/product subscribed to order processing: billing and customer care, service messages, roaming services, fraud detection, and technical issue resolution. Anonymous and de-identified data is collected to enhance service offerings and conduct surveys to gauge customer satisfaction and usage, network management, marketing, research and analytics without identifying individuals. Personal and traffic data are processed to prevent fraud, protect the network, and manage debts. However, in compliance with the data localization requirement under the Directive, no personal information is transferred outside the borders of Ethiopia by Safaricom Ethiopia.[191]

4.8. Compatibility of cross-border personal data transfer requirements of the Proclamation with international/ regional practices

The legislator has employed various approaches to impose data localization requirements in the Personal Data Protection Proclamation. As discussed in the previous Chapter about common forms of regulating cross-border data transfer, data localization is not limited to strict localization measures that restrict the transfer of data across borders; conditional cross-border data transfer requirements are criticized for being a disguised form of data localization.

The Proclamation adopts both strict and conditional forms of data localization. First, the data sovereignty requirement mandates that all personal data originating from Ethiopia must be stored

[190] Safaricom Telecommunications Ethiopia plc, Privacy Statement < https://safaricom.et/index.php/terms/privacy> accessed 13 October 2024

[191] ibid

on local servers. This type of localization requirement has been criticized for taking the regulation too far.[192] While it is possible to subsequently transfer a copy of the data to third-party jurisdictions by meeting the specified conditions, it is criticized as it increases the cost of digital trade by requiring additional resources and redundant investment.[193] Furthermore, for certain categories of critical personal data, the Proclamation prohibits cross-border processing altogether, which represents a strict data localization requirement. When defining the conditions that classify personal data as critical, the Proclamation references the strategic interests of the state, suggesting considerations beyond just privacy.

The Proclamation's strict data localization requirement is one of the key differences between it and the GDPR. Unlike the Proclamation, the GDPR does not impose data sovereignty or residency requirements. However, the conditions for data transfer, such as consent, necessity, or use in public databases, are similar in both the Proclamation and the GDPR. The adequacy test under the GDPR is comparable to the appropriateness test under the Proclamation, although the GDPR seems to assess a broader range of factors for verifying adequacy. Certain conditions recognized by the GDPR, such as binding corporate rules and appropriate safeguards, are not acknowledged in the Proclamation. Indirect localization could occur in both frameworks if the conditions for transfer cannot be met, effectively requiring the data to remain localized. The Proclamation seems to require pre-approval for almost all types of data transfers and prescreening by the Authority, this elongates the approval process and may be used as a strategy to discourage data transfers.

[192] Kholofelo Kugler (n 117)
[193] Alexander Beyleveld and Franziska Sucker (n 78)

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

I. CONCLUSION

The mere fact that the Proclamation has adopted a data sovereignty rule including strict data localization requirements for specified data sets should not lead to a conclusion that it has failed to create an enabling environment for the flourishment of digital trade and transformation. A useful insight can be gathered from the Proclamation's explanation note presented to HPR. The legislative intent behind developing a comprehensive data protection framework is to enable the country become beneficiary of the opportunities presented by digital transformation while answering for peculiar challenges that digitalization brings with it. The explanation note further reiterates the wordings of the Digital Ethiopia Agenda 2025, it recognizes the status of Ethiopia in the digitalization value chain as a digital 'late-starter' and emphasizes the need to build a data protection framework that works for the context of the country. It is in line with Digital Ethiopia Agenda 2025 that the priority for countries like Ethiopia is enhancing digital readiness. Amongst areas that the national strategy document wishes to improve with the aim of enhancing digital readiness is the ICT infrastructure. The strategy document does recognize that improvement work needs to be done to improve network coverage, uptake, affordability, and quality.[194] With this in mind, requiring all personal data originating from Ethiopia to be stored locally can be seen as a useful tool to develop the digital readiness and infrastructure of the country. Granted it's an additional cost for enterprises that are required to build large capacity data centers in Ethiopia where they already have a similar infrastructure somewhere else but unless the private sector is involved in enhancing the digital infrastructure of the country, similar to the benefits they wish to reap from data-driven technologies, opportunities from digital transformation will continue to suffer distributional inefficiencies. It's important to note that digital transformation is a journey. Countries like Ethiopia are in the first steps of the journey where the focus should be on enhancing digital readiness to fully appreciate the benefits of digital transformation.

i. Overview of the Proclamation in line with the AU DTS

[194] Digital Ethiopia 2025 (n 19)

It's imperative to review the Proclamation in line with the policy recommendation and proposed actions of the AU DTS. The continental strategy document has identified foundation pillars for digital transformation, the first pillar being creating an enabling regulatory and policy environment. The recommendation of the continental strategy document towards building the first pillar is for members to strengthen legislation on personal data for better control by data subjects.[195] In a country that had not had comprehensive personal data protection legislation, the introduction of a comprehensive cross-sectoral Personal Data Protection Proclamation on its own deserves appreciation and shows the state's commitment to implement the recommended actions under the continental strategy document.

Second, The DTS identifies cyber security, privacy & personal data protection among the cross-cutting themes necessary for building digital transformation. The action that is recommended by the Commission is for state parties to accelerate the establishment of Personal data protection Authorities.[196] A significant milestone in the Personal Data Protection Proclamation is the appointment of a new regulatory body for personal data protection, the Ethiopian Communications Authority. This is an extension of the mandate given to the ICT regulator under the Communications Services Proclamation. A discussion on this is made in Chapter 4, Section 4.6.

Furthermore, the AU DTS recommends African countries to adopt a law on localization of data with respects to privacy of African citizens and residents. [197]It further qualifies the recommendation by suggesting commercial rights or at least a fair commercial share from using African citizen's personal data to stay in Africa.[198] From this perspective, adopting a law that demanding local storage of personal data in local server or data centers does not go against the transformation agenda. This is also in line with the continental strategy document's recommendation to improve local content development and hosting in local servers and data centers.[199] Concerning non-personal data, the continental strategy document recommends state

[195] The Digital Transformation Strategy for Africa 2020-2030 (n 18)

[196] ibid

[197] ibid

[198] ibid 58.

[199] ibid 50.

parties develop regulations aimed at free flow of non-personal data. [200] The scope of the Personal Data Protection Proclamation is limited to personal data and there is no dedicated regulation thus far governing the cross-border flow of non-personal data. Practically, cross-border transfer of non-personal data is not frustrated as there is no legal restriction. However, the strategy document emphasized the need to develop intentional regulations to support the free flow of non-personal data.

ii. The Proclamation and the AfCFTA Digital Tarde Protocol

The principle is, so long as the transfer is to conduct digital trade, state parties should permit trans-boundary transfer of data. However, the exception dictates, restrictions to free flow of data can legitimately be imposed provided the four criteria set under the protocol are complied with. A restriction is legitimately imposed to trade-related cross-border data flow if it is to achieve a legitimate public policy objective, not arbitrary or unjustified, not meant as a disguised restriction on digital trade, and does not impose greater restriction than is required to achieve the objective.[201] When examined in line with the four criteria, the Proclamation does have areas that require improvement.

a) The Authority is given extensive discretion to restrict/ approve the request for cross border data transfer. Reading Article 20(1) of the Proclamation, a pre-approval is only required from the Authority where a transfer is made based on an assessment of appropriate level of protection in the third party jurisdiction or in case it entails transferring sensitive personal data as outlined under Article 22(3). This leaves room for a logical understanding that transfers made based on other conditions such as a limited form of transfer, based on Consent, necessity, or from public database are not dependent on obtaining the Authority's pre-approval and this is in line with the information obtained from the Authority. However, Article 48(1) of the Proclamation imposes obligation on Data Controllers/Processors to obtain prior authorization from the Authority before transferring the data to third-party jurisdictions. Similarly, Article 45(1) of the Proclamation requires a prior security check to be conducted by the Authority in case the Authority 'is of the opinion that the processing

[200] ibid13.

[201] AfCFTA Protocol on Digital Trade (n 20)

or transfer of data by a Data Controller or Data Processor may entail a specific risk to the privacy rights of data subjects'.

b) The Proclamation lacks predictability and transparency on how decisions to approve or reject transfer request are made. When a transfer is made based on appropriate protection test, a burden of proof is imposed on the Data Controller or Processor to demonstrate through evidence the recipient jurisdiction's appropriate level of protection. However, the Proclamation doesn't indicate the type of evidence the Data Controller or Processor must present to the Authority. furthermore, it requires proving general concepts such as the rule of law, professional rules, and security measures. In case the request is rejected, the Authority does not need to justify its decision. The lack of certainty extends to what is going to be labeled as critical personal data by the Authorities. There's a lot of unknowns here, what factors determine the categorization of personal data as critical? What is the demarcation between critical and sensitive personal data? Is all unknown and the Authority is working on subordinate legislation that will potentially answer for these questions. The Authority will consider factors beyond privacy in determining critical personal data which expands the grounds for restricting data transfer. There are also decisions left to the opinion of the Authority [202]with little to no indication of what informs the Authority's opinion. While the Proclamation has not yet been tested in practice, the Authority is given sufficient leeway to use the flexibilities in favor of restricting cross-border data transfer requests. Granting a broad spectrum of power to the Authority in determining what constitutes appropriate data transfer and the mandate to intervene with practically most data transfer requests will increase the likelihood of the decision being arbitrary and disguised restriction to digital trade falling short of the requirements set under the Protocol.

II. RECOMMENDATION

This research would like to conclude by making the following recommendations

i. **Creating a Regional/Continental ICT Value Chain**: This research has found that the data localization requirements under the Personal Data Protection Proclamation are intentionally designed to enhance digital readiness by developing local digital infrastructure. However, there

[202]Personal Data Protection Proclamation (n 93) art. 45(1)

should be room for revising these data localization requirements in the future to create an ICT value chain within the continent. If every African country requires data to be stored in its local data center, it could lead to redundancy and wasted investment. For each state to find its competitive advantage in ICT, African countries must come to a mutual understanding to develop a common cloud data center for storing less critical and less sensitive personal information. They should unite in improving connectivity, reducing the cost of ICT services and products, and enhancing ICT literacy in each state.

ii. **Private and Public Sector Collaboration in ICT Development**: Digital transformation is a shared objective among all players in the economy, both private and public. Industry actors should collaborate with local authorities to enhance digital readiness, even when it may not make commercial sense. Multinational organizations experienced in driving data-driven insights should work to transfer knowledge of data analysis to local talents, reducing the need to outsource analytics and data transfer.

Bibliography

Legal Materials

1. African Union Convention on Cyber Security and Personal Data Protection Adopted by the Twenty-Third Ordinary Session of the Assembly, Held in Malabo, Equatorial Guinea 27th June 2014 (Malabo Convention) [2014]
2. The Digital Transformation Strategy for Africa 2020-2030 (African Union)
3. Digital Ethiopia 2025: A Digital Strategy for Ethiopia Inclusive Prosperity (The Federal Democratic Republic of Ethiopia)
4. Communications Service Proclamation No.1148/2019
5. European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "Building a European Data Economy"' COM (2017) 9 final
6. Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade (Durban Feb. 2024) STC-JLA [2024]
7. Personal Data Protection Proclamation No. 1321/2024
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons With Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) [2016] L 119/1
9. SIM Cards Registration Directive No. 799/2021,
10. Telecommunications Consumer Rights and Protection Directive No. 832/2021
11. Telecommunications Quality of Service Directive No. 794/2021
12. Explanation notes to Personal Data Protection Proclamation No. 1321/2024

Articles and Journals

1. Beyleveld A. and Sucker F., *Cross-Border Data Flows in Africa: Policy Considerations for the AfCFTA Protocol on Digital Trade* (Mandela Institute 2022)
2. Carrière-Swallow Y. and Haksar V., *The Economics and Implications of Data: An Integrated Perspective* (International Monetary Fund 2019) Explanation notes to Personal Data Protection Proclamation No. 1321/2024

3. International Telecommunication Union and The World Bank, 'Data Protection and Trust' in Colin Blackman (ed), *Digital Regulation Handbook* (ITU Publications 2020)
4. International Telecommunication Union, 'Good Regulation Broadens Access and Ignites Markets' in K. Stimpson (ed), *Global ICT Regulatory Outlook 2020: Pointing the Way Forward to Collaborative Regulation* (3rd edn, ITU Publications 2020)
5. Information Technology and Global Governance, *Data Governance and Policy in Africa* (Bitange Ndemo and others (eds) Springer Nature 2023) 30.
6. Kugler K., T*he Impact of Data Localisation Laws on Trade in Africa* (Mandela Institute 2022)
7. Lemma A. and others, *The AfCFTA: Unlocking the Potential of the Digital Economy in Africa* (ODI report 2022)
8. Pisa M. and others, *Why Data Protection Matters for Development: The Case for Strengthening Inclusion and Regulatory Capacity* (CGD Note 2021)
9. The World Bank and The World Trade Organization, *Turning Digital Trade into a Catalyst for African Development* (The World Bank Group 2023)
10. Tekleselassie T., '*Developing Ethiopia's Digital Economy: Lessons from China'* [2021] ECIDC, Project Pape < Developing Ethiopia's Digital Economy: Lessons from China (unctad.org)> accessed 11 October 2024
11. UNCTAD, *Data Protection Regulations, and International Data Flows: Implications for Trade and Development* (United Nations 2016) 19.
12. Vial G. *Understanding Digital Transformation: A Review and a Research Agenda* (The Journal of Strategic Information Systems 2019)
13. Wickham Heath Consulting, *Cross-Border Data Flows Realizing Benefits and Removing Barriers* (GSMA 2018)

Websites

1. < https://etradeforall.org/news/new-wto-world-bank-project-seeks-to-boost-africas-participation-in-digital-trade/> accessed 12 June 2024
2. < https://explodingtopics.com/blog/data-generated-per-day> accessed 15 August 2024
3. < https://safaricom.et/index.php/terms/privacy> accessed 13 October 2024

Interviews

- Interview with Million H/Michael, Deputy Director General of the Ethiopian Communications Authority, August 2024

Interview Questions

- Is it required to obtain the Authority's pre-approval for all cross-border data transfers? In what context would Article 48(1), 45(1) of the Proclamation be applicable?
- Regarding Article 20(1), what types of evidence must a data controller or processor provide to demonstrate that an appropriate level of protection exists in third-party jurisdictions?
- For Article 19(2), what criteria will the Authority use to evaluate the presence of the rule of law in a third-party jurisdiction? What professional rules and security measures are mentioned in Article 20 of the Proclamation, and how can their existence be proven?
- Does the limited form of transfer under Article 19(3) of the Proclamation require the Authority's pre-approval? Does the Authority have the power to limit the scope of such transfers?
- Does Article 21 require obtaining the Authority's approval for every data transfer, even those based on consent or necessity made as per Article 20(1) (b), (c) and (d)?
- Under Article 22, what factors determine the categorization of personal data as critical? What are the strategic state interests mentioned in Article 22(2) of the Proclamation that guide the Authority in prescribing critical data categories?
- Does the Authority have a timeline for prescribing critical categories of personal data in accordance with Article 22 of the Proclamation?
- Is cross-border transfer prohibited for **critical personal data?**
- What is the implication of the data sovereignty clause under Article 22(1) in restricting cross-border data transfers? can a copy of the data stored locally be transferred across borders provided the conditions for the transfer are met?