

**Beyond the GDPR: Culturally-Contextualized Privacy and Data Protection in Africa's
Expanding Digital Landscape**

Dianah Ajuna

Thesis submitted to the University of Ottawa
in partial Fulfillment of the requirements for the
Doctor of Philosophy (Ph.D.) Degree in Law

Faculty of Law
University of Ottawa

© Dianah Ajuna, Ottawa, Canada, 2025

Abstract

This thesis explores the intersection of privacy, data protection, and African cultural values within the continent's dynamic digital landscape. Using Africa's socio-economic realities and collective values as a foundation, it critiques the limitations of European privacy and data protection models, particularly the European General Data Protection Regulation (GDPR), in fully meeting Africa's unique regulatory needs. Through a legal doctrinal analysis and the Third World Approaches to International Law (TWAIL) framework, this thesis examines how colonial legacies have influenced global privacy and data protection governance, often imposing individualistic norms that neglect Africa's communal principles of privacy, which include and emphasize collective well-being over solely focusing on individual rights. The findings identify three primary challenges associated with directly implementing GDPR standards in Africa: 1) misalignment with African communal values that prioritize shared interests; 2) impracticality of compliance due to limited resources and infrastructure; and 3) neocolonial pressures that limit Africa's regional sovereignty in shaping its privacy and data protection governance. Assessing frameworks like the African Union's Malabo Convention, the thesis identifies barriers in regional implementation and enforcement.

To address these challenges, the thesis proposes a culturally sensitive, decentralized model for privacy and data protection, integrating African values to balance individual rights with communal interests while enhancing local empowerment in regulatory decisions. The proposed model integrates concepts such as relational consent, data custodianship, and collective privacy rights, emphasizing flexible, decentralized, and community-responsive regulation. This approach provides a normative and practical alternative to externally imposed models, enhancing local ownership and regulatory legitimacy. This thesis contributes a decolonized, contextually relevant framework for privacy and data protection,

offering policymakers a roadmap to strengthen Africa's privacy and data protection sovereignty and foster inclusive, equitable privacy and data protection governance in the digital age.

Table of Contents

ABBREVIATIONS.....	VII
ACKNOWLEDGEMENTS	X
1 CHAPTER 1: GOALS AND OBJECTIVES.....	1
1.1 CONTEXT	1
1.2 EUROPEAN INFLUENCE ON DATA PRIVACY IN AFRICA	4
1.3 COLONIAL INFLUENCE ON REGIONAL DATA PRIVACY	5
1.4 OVERVIEW OF AFRICAN DATA PROTECTION LEGISLATION.....	6
1.5 THE SIGNIFICANCE OF TWAIL IN SHAPING AFRICA’S DATA PROTECTION LANDSCAPE	8
1.6 CONTEXTUALIZING PRIVACY AND DATA PROTECTION	10
1.7 PROBLEM STATEMENT	12
1.8 PURPOSE OF THE STUDY.....	13
1.9 SPECIFIC RESEARCH OBJECTIVES.....	13
1.10 RESEARCH QUESTIONS.....	13
1.11 THESIS STATEMENT.....	14
1.12 THESIS ARGUMENT.....	14
1.13 WHY AFRICA AS ONE BLOC?.....	15
1.14 METHODOLOGY.....	17
1.15 SIGNIFICANCE, JUSTIFICATION, AND SCOPE OF THE STUDY	19
1.16 CHAPTER SYNOPSIS	22
2 CHAPTER TWO: LITERATURE REVIEW AND THEORETICAL FRAMEWORK	25
2.1 INTRODUCTION	25
2.2 LITERATURE REVIEW.....	27
2.2.1 <i>Evolving Perspectives on Privacy in the African Context.....</i>	<i>30</i>
2.2.2 <i>Definition of Privacy in Africa</i>	<i>34</i>
2.2.3 <i>Culture, privacy, and data protection.....</i>	<i>36</i>
2.2.4 <i>Religion, Privacy, and Data Protection</i>	<i>39</i>
2.2.5 <i>Developmental Priorities, Privacy, and Data Protection</i>	<i>41</i>
2.2.6 <i>The Intersection of Technology, Privacy, and Data Protection in Africa</i>	<i>42</i>
2.2.7 <i>Evolution of laws on privacy and data protection in Africa</i>	<i>43</i>
2.3 THEORETICAL FRAMEWORK.....	46
2.3.1 <i>Navigating Through TWAIL and the Legacy of Colonialism</i>	<i>49</i>
2.3.2 <i>TWAIL’s Critique of Eurocentrism.....</i>	<i>51</i>
2.3.3 <i>Dependency Theory.....</i>	<i>54</i>
2.3.4 <i>Human Rights and Social Justice</i>	<i>58</i>
2.4 CONCLUSION	61
3 CHAPTER 3: COMPLEXITIES OF TRANSPLANTING GDPR INTO AFRICAN LEGAL FRAMEWORKS63	
3.1 INTRODUCTION	63
3.2 OVERVIEW OF THE GDPR.....	70
3.2.1 <i>Evaluating the Economic Impact of GDPR Non-Compliance on Diverse Entities</i>	<i>76</i>
3.2.2 <i>Exploring the Economic Impact of GDPR on Africa</i>	<i>77</i>
3.3 LEGAL CHALLENGES: A CONFLICT BETWEEN THE GDPR AND LOCAL LEGAL FRAMEWORKS	79
3.4 CULTURAL DISTINCTIONS: GDPR ADOPTION CHALLENGES IN AFRICA.....	85
3.5 FINANCIAL AND TECHNOLOGICAL ROADBLOCKS TO GDPR COMPLIANCE IN AFRICA.....	91
3.6 INSTITUTIONAL CHALLENGES IN UPHOLDING GDPR-INSPIRED LEGISLATION IN AFRICA	97
3.7 CHALLENGES IN HARMONIZING DATA PROTECTION LEGISLATION ACROSS AFRICA: A REVIEW OF REGIONAL EFFORTS AND IMPLEMENTATION HURDLES	101
3.7.1 <i>Challenges of Implementing Transplanted GDPR Standards in ECOWAS Member States</i>	<i>102</i>

3.7.2	<i>Challenges of Implementing Transplanted GDPR Standards in SADC Member States</i>	104
3.7.3	<i>Challenges of Implementing Transplanted GDPR Standards in East African Countries. ..</i>	106
3.7.4	<i>Challenges of Implementing Transplanted GDPR Standards in ECCAS Member States ..</i>	109
3.7.5	<i>Challenges of Implementing Transplanted GDPR Standards in Arab Maghreb Union Member States</i>	112
3.7.6	<i>Enduring Gaps in Implementation.....</i>	113
3.8	CONCLUSION	114
4	CHAPTER 4: EVALUATING AFRICAN UNION AND REGIONAL ORGANIZATIONS' EFFORTS IN DATA PROTECTION AND PRIVACY.....	116
4.1	INTRODUCTION	116
4.2	CONSTITUTIONAL FOUNDATIONS AND DEVELOPMENTS IN PRIVACY AND DATA PROTECTION ACROSS AFRICA	121
4.2.1	<i>African Human Rights Frameworks: Data Protection and Privacy Considerations</i>	124
4.2.2	<i>An overview of African Countries with privacy and data protection legislation</i>	126
4.2.3	<i>European Influence and International Commitments in African Privacy and Data Protection Legislation</i>	129
4.3	THE MALABO CONVENTION: A COMPREHENSIVE LEGAL FRAMEWORK FOR CYBER SECURITY AND DATA PROTECTION IN AFRICA.....	132
4.3.1	<i>Data Protection Framework of the Malabo Convention</i>	135
4.3.2	<i>Influence of the Convention on National Legal Frameworks</i>	138
4.3.3	<i>Strategic Advancements in Digital Governance: The African Union's Data Policy Framework</i>	140
4.4	PRIVACY AND DATA PROTECTION INSTRUMENTS OF AFRICAN REGIONAL ECONOMIC COMMUNITIES (RECs)	144
4.4.1	<i>Regional Integration and Data Protection Initiatives in The Economic Community of West African States (ECOWAS).....</i>	146
4.4.2	<i>Regional Adaptations in Data Protection: Comparing the AU Malabo Convention and ECOWAS Supplementary Act</i>	148
4.4.3	<i>Data Protection Laws Enacted within the ECOWAS Region</i>	150
4.4.4	<i>Data Protection and Privacy Laws in the Southern African Development Community (SADC): Influence of European Standards.....</i>	153
4.4.5	<i>Advancements in SADC Data Protection Legislation: HIPSSA Model Laws and European Influence</i>	156
4.4.6	<i>Data Protection Progress in the East African Community: EU Influence and Local Developments.....</i>	159
4.4.7	<i>Data Protection Evolution in Central Africa: ECCAS and CEMAC's Model Laws.....</i>	161
4.4.8	<i>Data Privacy Legislation and Influences in North Africa: Progress and Challenges</i>	164
4.5	ADAPTING GLOBAL DATA PRIVACY STANDARDS IN AFRICA: EUROPEAN INFLUENCE AND REGIONAL VARIABILITY	166
4.6	CONCLUSION	169
5	CHAPTER 5: CULTURALLY CONTEXTUALIZING PRIVACY AND DATA PROTECTION: AN AFRICAN APPROACH TO REGULATION AND GOVERNANCE.....	172
5.0	INTRODUCTION	172
5.1	APPROACHES TO REGULATION OF PRIVACY AND DATA PROTECTION	174
5.1.1	<i>Individual Rights-Based Approach to Privacy and Data Protection</i>	177
5.1.2	<i>Traditional Governance Approach to Privacy Regulation</i>	181
5.1.3	<i>The Regulation Approach to privacy and data protection</i>	184
5.1.4	<i>Culturally Contextual approach to privacy and data protection</i>	187
5.2	CULTURAL FOUNDATIONS OF PRIVACY AND DATA PROTECTION	194
5.2.1	<i>Balancing Individual and Communal Interests in African Privacy and Data Protection Frameworks.</i>	197
5.2.2	<i>Community-Centric Privacy and Data Protection: Lessons from Indigenous Practices ...</i>	202
5.2.3	<i>Collective Approach</i>	204
5.2.4	<i>Integrating African Cultural Perspectives into Privacy and Data Protection Frameworks .</i>	208

5.3	A NEW PARADIGM FOR PRIVACY AND DATA PROTECTION IN AFRICA	210
5.3.1	<i>Ownership in Social Contexts: Individual and Collective Perspectives</i>	210
5.3.2	<i>Integrating Collective Ownership into Privacy and Data Protection Frameworks</i>	214
5.3.3	<i>Redefining the Principle of Access in Privacy and Data Protection Frameworks</i>	219
5.3.4	<i>Decentralizing Data Protection Mechanisms: A Community-Driven Approach</i>	224
5.4	DATA STEWARDSHIP IN AFRICAN COMMUNAL CONTEXTS: A MODEL FOR PRIVACY AND PROTECTION	227
5.5	COLONIAL INFLUENCES ON AFRICAN CUSTOMARY LAW AND PRIVACY FRAMEWORKS	229
5.5.1	<i>Colonial Perspectives on African Customary Law</i>	232
5.5.2	<i>The Marginalization and Transformation of Customary Law in Colonial Africa</i>	235
5.6	ADDRESSING ECONOMIC DISPARITIES AND RESOURCE CONSTRAINTS IN DATA PROTECTION FOR AFRICAN COUNTRIES	238
5.7	CONCLUSION	241
6	CHAPTER 6: CONCLUSION, RESEARCH IMPLICATIONS, AND POLICY RECOMMENDATIONS. 245	
6.0	INTRODUCTION	245
6.1	SUMMARY OF THE FINDINGS	248
6.1.1	<i>Challenges of Implementing the GDPR in Africa</i>	248
6.1.2	<i>Contextual Misalignment of GDPR with African Realities</i>	250
6.1.3	<i>Regulatory Burdens and Economic Implications</i>	253
6.1.4	<i>The Necessity of Contextual Adaptation in Data Protection for Africa</i>	255
6.2	EXISTING MECHANISMS AND FRAMEWORKS IN AFRICA.....	257
6.2.1	<i>Challenges of Harmonization and Enforcement</i>	258
6.2.2	<i>The Dominant External Influence on African Data Protection Laws: A Continuation of Colonial Legacies</i>	260
6.2.3	<i>African Philosophical Values and Data Protection Laws</i>	263
6.3	THE NEED FOR CULTURALLY CONTEXTUALIZED ADAPTATION IN PRIVACY AND DATA PROTECTION	264
6.3.1	<i>Recognition of Group and Collective Data Rights</i>	267
6.3.2	<i>Traditional Dispute Resolution Mechanisms</i>	268
6.3.3	<i>Frameworks in Local Languages and Accessible Formats</i>	269
6.3.4	<i>Contextualized Compliance Mechanisms</i>	269
6.4	IMPLICATIONS OF THE RESEARCH	270
6.4.1	<i>Contextualization of Privacy and Data Protection Frameworks</i>	270
6.4.2	<i>Policy Development and Legal Reform</i>	271
6.4.3	<i>Contribution to Academic Discourse and Theoretical Development</i>	271
6.5	RECOMMENDATIONS	272
6.5.1	<i>Moving Beyond GDPR: Developing Culturally Relevant Data Protection Laws</i>	272
6.5.2	<i>Regional Harmonization and Legal Cooperation</i>	273
6.5.3	<i>Integrating African Cultural Values into Legal Frameworks</i>	274
6.6	CONCLUSION AND FUTURE PATHWAYS	274
6.6.1	<i>Call to action</i>	275
7	BIBLIOGRAPHY	276

Abbreviations

ACHPR	African Charter on Human and Peoples Rights
ACHR	African Charter on Human Rights
AFAPDP	African Framework for Data Protection
AHRC	African Human Rights Commission
ANSICE	National Agency for Information System Security (Agence Nationale de la Sécurité des Systèmes d'Information)
APD	Autorité de Protection des Données (Data Protection Authority)
APDP	Autorité de Protection des Données Personnelles (Personal Data Protection Authority)
AU	African Union
BPO	Business Process Outsourcing
CDP	Commission for Data Protection
CEMAC	Economic and Monetary Community of Central Africa (Communauté Économique et Monétaire de l'Afrique Centrale)
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CIL	Customary International Law
CMIL	Colonial and Modern International Law
CNIL	Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority)
CNPD	Comissão Nacional de Protecção de Dados (Portuguese Data Protection Authority)

CNPDCP	Commission Nationale de Protection des Données à Caractère
Personnel	(National Commission for the Protection of Personal Data)
COMESA	Common Market for Eastern and Southern Africa
DNA	Deoxyribonucleic Acid
DPA	Data Protection Authority
DPC	Data Protection Commissioner
DPD	Data Protection Directive
DSM	Digital Single Market
EAC	East African Community
EC	European Commission
ECCAS	Economic Community of Central African States
ECOWAS	Economic Community of West African States
EDPB	European Data Protection Board
EEA	European Economic Area
EU	European Union
EUR	Euro (Currency)
GDPR	General Data Protection Regulation
HAPDP	Harmonized African Personal Data Protection
HIPSSA	Harmonization of ICT Policies in Sub-Saharan Africa
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
ID	Identity Document
IDPC	International Data Protection Commissioners
IGAD	Intergovernmental Authority on Development
II	Information Infrastructure

IMF	International Monetary Fund
INPDP	Instance Nationale de Protection des Données Personnelles (National Instance for the Protection of Personal Data)
IPDCP	International Programme for Data Protection and Cybersecurity
IR	International Relations
IT	Information Technology
ITU	International Telecommunication Union
LED	Law Enforcement Directive
NAPP	National Authority for Personal Protection
NAPPD	National Agency for the Protection of Personal Data
NDPA	National Data Protection Authority

Acknowledgements

Above all, I thank God for His unwavering grace and strength that carried me through every step of this journey. I am also deeply thankful to my supervisors, Professors Chidi Oguamanam and Jeremy de Beer, for their tireless guidance, kind mentorship, and steadfast belief in my work, they supported me to the end and believed in me. I remain grateful to Professor Vivek Hariharan Krishnamurthy, who journeyed with me through the early stages and offered invaluable insights during the proposal phase. Further, my gratitude extends to the exceptional team of examiners, Professors Anita L. Allen, Caroline Ncube, Teresa Scassa, and Vivek Hariharan Krishnamurthy, for their insightful and detailed comments.

Alongside this, my sincere appreciation goes to the Open African Innovation Research (Open AIR) family for walking this journey with me, and to the Canadian Queen Elizabeth Advanced Scholars program for their generous financial support. I gratefully acknowledge the support from the P.E.O. International Peace Scholarship. Equally, I am grateful to Nkumba University and Uganda Christian University for giving me the opportunity to teach, which motivated this journey. On a practical note, I thank Richard Ssekitoleko for his technical support; James and Helen Lunney, who became family and made Canada feel like home; and all my home community members who kept encouraging me along the way. To my dear friends, thank you for your prayers, encouragement, and for cheering me on.

Finally, though by no means least, my heartfelt gratitude goes to my family; without them, I would not have made it, they were my strength. My precious daughter, Isabella, kept me going and excited about each step. My loving parents, Professor Christopher Byaruhanga and Christine Byaruhanga, offered generous support, a steady presence, and unending love throughout this project. My brothers, Dixon and Dan, believed in me, supported me and

cheered me on. Hope and Nakabiito, together with my nieces and nephews, Timothy, Tabitha, Krista, Victor, Murungi, and Alinda, prayed continually. I am also thankful to Trevor for being a source of strength when I needed it most.

In remembrance, this work is dedicated to the memory of my beloved son, Aaron Tugume, who went to be with the Lord on May 3, 2021, and my loving grandmother, Evanis Katongole, who went to be with the Lord on June 1, 2021.

Chapter 1: Goals and Objectives

1.1 Context

The digital transformation in Africa has been significantly shaped by the rapid expansion of internet access and the increasing penetration of mobile technologies. According to the After Access 2022 Survey conducted by Research ICT Africa, internet usage in South Africa had reached 75% by 2022,¹ while Ethiopia saw growth from just 3% in 2012 to 16% by 2022,² and Uganda recorded a penetration rate of 18% in the same year.³ These advances have been driven by factors such as the expansion of telecommunications infrastructure, widespread availability of affordable smartphones, and targeted efforts by governments and international partners to bridge the digital divide.⁴ Despite these positive trends, significant disparities persist across the continent. For example, Ethiopia's internet penetration remains below the 20% threshold typically associated with the economic benefits of digital inclusion, while in Uganda, many remain offline due to limited awareness and affordability challenges.⁵ These gaps not only reflect uneven access but also raise pressing concerns about whether current regulatory frameworks for privacy and data protection are adequately equipped to regulate a rapidly evolving digital space. As the continent's digital domain continues to expand, the need for regulatory responses that are not only technically robust but also contextually and culturally grounded becomes increasingly urgent.

¹ Research ICT Africa, *Digital Africa Post the Pandemic: South Africa Report (After Access 2022–2023)*, online: <https://researchictafrica.net/research/digital-africa-post-the-pandemic-south-africa-report-after-access-2022-2023/>.

² Research ICT Africa, *Internet Development in Ethiopia: High-Level Findings from the After Access Survey*, online: <https://researchictafrica.net/research/internet-development-in-ethiopia-high-level-findings-from-the-after-access-survey/>.

³ Research ICT Africa, *After Access 2022: Internet Usage Trends in Uganda*, online: <https://researchictafrica.net/research/after-access-2022-internet-usage-trends-in-uganda/>.

⁴ Alan Mauldin, International Internet Capacity Growth Just Accelerated for the First Time Since 2015, Telegeography (Sept. 20, 2018) <https://blog.telegeography.com/international-internet-capacity-growth-just-accelerated-for-the-first-time-since-2015>.

⁵ Research ICT Africa, *After Access 2022 Survey*, online: <https://researchictafrica.net/project/after-access-2022-survey/>.

Simultaneously, on a global scale, the GDPR⁶ has swiftly emerged as the predominant standard for data protection laws since its implementation in 2018. The genesis of this regulation can be traced to a recognition within the European Union (EU) that the prevailing regulatory framework, as articulated in the Data Protection Directive (DPD)⁷, proved inadequate in addressing the escalating threats to the privacy rights of European citizens.⁸ The DPD further exacerbated inconsistencies among the data protection laws of EU Member States, leading to heightened complexities.⁹ While the GDPR has gained praise for prioritizing users and their digital privacy needs, it is crucial to acknowledge the nuanced perspectives that arise when considering its implementation in Africa. The GDPR is acclaimed for placing a user-centric approach at its core. It reflects a consensus rooted in European norms and values, primarily addressing the concerns and rights of European users.¹⁰ This context sets the stage for an in-depth exploration of the mixed reactions sparked by the adoption of the GDPR model in Africa. Divergent viewpoints among experts and policymakers highlight a complex environment where the perceived advantages of comprehensive data protection legislation must be weighed against concerns about cultural misalignment and potential implications for individuals in Africa. The ensuing dialogue highlights the intricate interplay between global regulatory frameworks and their adaptability to diverse regional contexts.

In light of the complexity stated above, acknowledging the necessity for a comprehensive approach, the African Union (AU) has taken significant strides in regulating

⁶ Council Regulation (EU) 2016/679 of the European Parliament and of the Council of 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 O.J. (L 119) 1 [hereinafter GDPR].

⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter DPD].

⁸ Foo Yun Chee, Yet to Show Its Teeth, Landmark EU Privacy Law Already a Global Standard, Reuters (May 22, 2019) <https://www.reuters.com/article/idUSKCN1SS1JU/>.

⁹ *Ibid.*

¹⁰ Makulilo, A B. "Data Protection Regimes in Africa: Too far from the European 'Adequacy' Standard?" (2012) 3:1 International Data Privacy Law 42.

privacy and data protection across the continent. Adopting the African Union Convention on Cyber Security and Personal Data Protection, also known as the Malabo Convention, in 2014 marks a crucial step in promoting a secure cyber environment and safeguarding personal data in Africa. Many African countries have also enacted national legislation to regulate privacy and data protection, such as Kenya's Data Protection Act¹¹ and Nigeria's Data Protection Regulation.¹² However, the effectiveness of these initiatives is yet to be fully realized, raising concerns about the enforcement and implementation mechanisms.¹³ While progress has been made, addressing the issue of privacy and data protection in Africa requires collaborative efforts at both the continental and regional levels, as national laws often have limited impact beyond borders. Despite the existence of regional instruments such as the ECOWAS Supplementary Act on Personal Data Protection,¹⁴ SADC Model Law on Data Protection,¹⁵ EAC Cyber laws, and African Personal Data Protection Guidelines,¹⁶ the overall status of legal protection for privacy and data protection in Africa remains to be determined.¹⁷

To bridge the gap and address the unique challenges of Africa's digital landscape, this thesis aims to contextualize privacy and data protection within African cultural perspectives. The objective is to develop culturally relevant and effective privacy and data protection frameworks that resonate with Africa's diverse populations and cultural contexts. Through this exploration, the thesis seeks to contribute to the ongoing development of comprehensive and inclusive privacy and data protection frameworks in Africa, ensuring the preservation of

¹¹Kenya Law. (2019). Data Protection Act, 2019. Retrieved from http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/DataProtectionAct_No24of2019.pdf.

¹² Nigeria Data Protection Regulation. (2019). Retrieved from <https://www.nitda.gov.ng/wp-content/uploads/2019/01/Nigeria-Data-Protection-Regulation-2019.pdf>.

¹³ Udoh, Victoria & David Ademola Olajide. "Data Protection in Nigeria: A review of the Nigerian Data Protection Regulation 2019 and the need for Nigeria to sign the African Convention on Data Protection" (2021) SSRN Electronic Journal.

¹⁴ Economic Community of West African States. (2010). Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS. Retrieved from <https://www.ecowas.int/wp-content/uploads/2019/07/Supplementary-Act-on-Personal-Data-Protection.pdf>.

¹⁵ Southern African Development Community. (2009). Model Law on Data Protection. Retrieved from https://www.sadc.int/files/9113/5292/8367/Model_Law_on_Data_Protection.pdf.

¹⁶ East African Community. (2014). EAC Cyber Laws. Retrieved from <https://www.eac.int/sites/default/files/docs/2014%20-%20EAC%20Cyber%20Laws.pdf>.

¹⁷ Makulilo, Alex B. "African Data Privacy Laws" (2016) Law, Governance and Technology Series.

privacy rights in the digital age. Drawing inspiration from the African Union's initiatives in privacy and data protection regulation, this thesis adopts the TWAIL lens to analyze Africa's most effective regulatory approaches. In doing so, it explores the potential for a cohesive African continental regulatory framework that can provide a unified and contextually sensitive approach to privacy and data protection across the continent. This approach seeks to balance the protection of individual privacy rights with the socio-cultural values of Africa's diverse populations, offering a more comprehensive solution tailored to Africa's unique digital challenges.

1.2 European Influence on Data Privacy in Africa

This section provides the historical and structural context for understanding why the GDPR wields considerable influence beyond Europe. In understanding the regulatory framework in Africa, it is essential to examine the evolution of European data protection regulations. From the introduction of Article 25 in the DPD¹⁸ in the 1990s to the establishment of the GDPR as its replacement, a significant shift is observed. While the DPD obligated EU member states to ensure the application of personal data legislation in non-EU countries, the GDPR, with its direct binding applicability, transferred the responsibility for safeguarding the data of EU individuals processed outside the EU to the countries where the processing occurs, as highlighted in Article 3.¹⁹ This comparison sets the stage for analyzing the influence of European regulations on privacy and data protection in Africa, providing a foundation for assessing the relevance and adaptability of these frameworks in light of Africa's distinct socio-legal contexts.

Consequently, the evolution of European data protection law has exerted a far-reaching impact, shaping perceptions of regulatory standards not only within the EU but also

¹⁸ See DPD, *supra* note 7, at art. 25.

¹⁹ GDPR, *supra* note 6, at art. 3.

globally.²⁰ In the African context, both the DPD and the GDPR have come to serve as normative benchmarks for regional legal frameworks.²¹ Within Africa, the AU Convention on Cyber Security and Personal Data Protection (Malabo, 2014) entered into force in 2023, but its regulatory influence remains constrained by limited ratifications, slow domestication, and uneven institutional capacity across Member States. By contrast, the ECOWAS Supplementary Act A/SA.1/01/10 (2010) has shown greater practical traction in West Africa, informing national legislation and DPA practice, though implementation still varies by state.²² Similarly, the SADC Model Law (2013) is emerging as a reference point for data protection developments in other parts of sub-Saharan Africa.²³

Examining these influences reveals distinctions between European and African approaches to data protection. European instruments represent three generations of data privacy law development, with the GDPR being the latest iteration. In contrast, the three principal African multilateral instruments, the ECOWAS Supplementary Act, the AU Convention, and the SADC Model Law, lack a distinct Africa-specific approach and exhibit an absence of communitarian African cultural discourse.²⁴ The African instruments, incorporating elements from the DPD, have also integrated standards from the GDPR.²⁵ Notably, a detailed discussion on this integration will follow in the subsequent chapters of the thesis, highlighting the interaction between global and regional regulatory dynamics.

1.3 Colonial Influence on Regional Data Privacy

European influence on African privacy and data protection frameworks is not something new. It is rooted in colonial legal and economic structures. The complex network

²⁰ Foo Yun Chee, *supra* note 8.

²¹ Alex B. Makulilo, The Future of Data Protection in Africa, in *African Data Privacy* 371, 377 (Alex B. Makulilo ed., 2016).

²² *Ibid.*

²³ *Ibid.*

²⁴ *Ibid.*

²⁵ Dominic N. Dagbanja, The Right to Privacy and Data Protection in Ghana, in *African Data Privacy Laws* 229, 231 (Alex B. Makulilo ed., 2016).

of economic connections between Europe and Africa, highlighted by the EU's role as the largest trading partner of Sub-Saharan Africa, has deep historical roots in colonialism. While globalization has intensified interdependence between regions, the structural asymmetries underpinning these relationships continue to reflect enduring colonial legacies.²⁶ The EU holds a notable position in Sub-Saharan Africa, contributing to a substantial portion of both imports and exports.²⁷ The enduring impact of colonial legal foundations is apparent, as indigenous populations were required to adopt legal systems shaped by continental European powers or British common law during the colonial era.²⁸ Despite the formal independence of African nations from contemporary European laws, the historical ties persist, evident through the influence of EU legislation and the laws of specific EU Member States.²⁹

In the realm of privacy and data protection standards, Article 25 of the DPD serves as a mechanism for post-colonial blocs to perpetuate European influence in Africa. For instance, Conventions like the 2013 Francophone Binding Corporate Rules play a role in aligning data privacy laws of former French colonies in northwest Africa with those of France.³⁰ Furthermore, the French data protection authority, *Commission Nationale de l'Informatique et des Libertés (CNIL)*, actively contributes technical expertise to enhance data privacy in these regions.³¹ Similarly, this pattern is not unique, as Portuguese influence is discernible in the data protection laws of Cape Verde and its other former colonies.³²

1.4 Overview of African Data Protection Legislation

²⁶ Dhruv Gandhi, Figure of the Week: Africa's New Trading Partners, Brookings (Mar. 7, 2018), <https://perma.cc/TQC6-TVWQ>.

²⁷ African Countries Are Building a Giant Free-Trade Area, Economist (Dec. 7, 2017), <https://perma.cc/2YGX-5QJJ>.

²⁸ Sandra Fullerton Joireman, Inherited Legal Systems and Effective Rule of Law: Africa and the Colonial Legacy, 39 J. Mod. Afr. Stud. 571, 576 (2001).

²⁹ *Ibid.*

³⁰ Cynthia O'Donoghue, Francophone Data Protection Authorities Postpone Adoption of a New Framework for International Data Transfers, Tech. Law Dispatch (Mar. 29, 2013), <https://perma.cc/3997-37JM>.

³¹ The CNIL Worldwide, CNIL, <https://perma.cc/2VNG-E6ZG>.

³² João Luís Traça & Bernardo Emrby, An Overview of the Legal Regime for Data Protection in Cape Verde, 1 Int'l Data Priv. L. 249, 251 (2011).

In the subsequent chapters, I explore in detail African data protection legislation. Over the past decade, multinational African conferences have been convened to deliberate on continental standards for personal data protection, aiming to achieve harmonization of norms across the region.³³ As a result, these discussions have resulted in the establishment of four data protection frameworks at both regional and sub-regional levels. Specifically, these frameworks encompass the AU Convention on Cybersecurity and Personal Data Protection 2014,³⁴ the ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection,³⁵ the SADC Data Protection Model Law 2012,³⁶ and the EAC Legal Framework for Cyber Laws 2008 (Phase I).³⁷ Additionally, a noteworthy development in the mid-2010s was the formulation of the African Declaration on Internet Rights and Freedoms, crafted through extensive multi-stakeholder involvement.

However, among the instruments that require ratification, none has secured ratification by a majority of Member States, shifting the focus to national legislation as the central point of ongoing efforts. To date, thirty-six out of fifty-four African countries have data protection laws and/or regulations. Nineteen countries have signed the African Union Convention on Cyber Security and Personal Data Protection adopted on 27 June 2014 (Malabo Convention), and fifteen countries have ratified it.³⁸ This dynamic between regional and national initiatives provides an essential foundation for the analysis of African privacy and data protection legislation in the subsequent chapters, shedding light on the challenges

³³ Alex B. Makulilo, The Future of Data Protection in Africa, in *African Data Privacy Laws* 371, 377 (Alex B. Makulilo ed., 2016).

³⁴ African Union Convention on Cyber-security and Personal Data Protection (27 July 2014) retrieved from <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

³⁵ Economic Community of West African States. (2010). Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS. Retrieved from <https://www.ecowas.int/wp-content/uploads/2019/07/Supplementary-Act-on-Personal-Data-Protection.pdf>.

³⁶ Southern African Development Community. (2009). Model Law on Data Protection. Retrieved from https://www.sadc.int/files/9113/5292/8367/Model_Law_on_Data_Protection.pdf.

³⁷ East African Community. (2014). EAC Cyber Laws. Retrieved from <https://www.eac.int/sites/default/files/docs/2014%20-%20EAC%20Cyber%20Laws.pdf>.

³⁸ Lovells, Hogan, "Recent developments in African data protection laws - Outlook for 2023", *Lexology* (24 February 2023), online: <https://www.lexology.com/library/detail.aspx?g=baef72ee-10bd-4eb9-a614-a990c236bb45#:~:text=To%20date%2C%20thirty%20six%20out,protection%20laws%20and%20For%20regulations>.

and progress in achieving a comprehensive and harmonized privacy and data protection framework across the continent.

1.5 The Significance of TWAIL in Shaping Africa's Data Protection Landscape

In the context of this intricate interplay between regional and national endeavours, the significance of TWAIL emerges as a pivotal lens through which to comprehend and address the multifaceted challenges that Africa grapples with, rooted in colonial legacies, neocolonial influences and global economic disparities. Specifically, originating as a critical legal theory in the 1990s, TWAIL confronts the Eurocentric perspectives ingrained in international law, advocating for a more nuanced understanding that incorporates the historical, social, and economic realities of countries in the Global South, prominently including Africa.³⁹ In this regard, it highlights the enduring impacts of colonialism and neocolonialism on the African continent.⁴⁰ Consequently, this connection between regional and global perspectives sets the stage for a comprehensive analysis of Africa's privacy and data protection regime, considering both the local and international dimensions that shape its development and challenges.

The historical context reveals Africa's enduring struggle against economic disparities in global affairs, where its resources have been consistently exploited by foreign entities.⁴¹ Likewise, this economic inequality extends into the digital realm, with global tech companies and data-driven corporations from outside Africa exercising control over the collection, processing, and utilization of African data.⁴² In addition, the digital divide further amplifies

³⁹ Makau Mutua & Anghie Antony, "What is TWAIL?" (2000) 94 Cambridge University Press on behalf of the American Society of International Law 31–40.

⁴⁰ *Ibid.*

⁴¹ Antony Anghie, "The Evolution of International Law: Colonial and postcolonial realities" (2006) 27:5 Third World Quarterly 739–753.

⁴² Kwet, M. (2019). "Digital colonialism: US empire and the new imperialism in the Global South." *Race & Class*, 60(4), 3-26. <https://doi.org/10.1177/0306396818823172>.

these disparities, with nations possessing superior digital capabilities exerting greater influence over their data and shaping global data policies.⁴³ Furthermore, these external powers often impose privacy standards that fail to align with African cultural and societal norms, thereby deepening the divide in terms of privacy protections.

Correspondingly, a core tenet of TWAIL involves the call for decolonizing legal and governance systems, acknowledging the importance of local knowledge, cultural norms, and community involvement in implementing effective measures.⁴⁴ In particular, this aligns seamlessly with ongoing efforts to counteract data colonialism across Africa, where foreign entities often control the collection, processing, and management of African data, impeding the efficient use and benefit of African nations.⁴⁵ Thus, TWAIL's call for decolonization encompasses reclaiming data and privacy sovereignty, empowering African nations to assert control over both their data and privacy and formulating comprehensive data protection and privacy policies that prioritize the best interests of their citizens.

Given Africa's historical experiences of colonialism, neocolonialism, and economic disparities, TWAIL provides invaluable insights into the power dynamics and structural inequalities influencing data governance and privacy protection. By critically examining historical forces shaping legal systems and institutions, TWAIL exposes power imbalances between African countries and global players dominating the data economy⁴⁶ and imposing privacy standards that may not suit the African context. As a result, this critical analysis enhances the understanding of how data and privacy-rich countries and entities

⁴³ *Ibid.*

⁴⁴ Luis Eslava and SundhyaPuhuja, "Beyond the (Post)Colonial: TWAIL and the Everyday Life of International Law" (2012) 45:2 Law and Politics in Africa, Asia and Latin America 195-221 at 217.

⁴⁵ Sandra Fullerton Joireman, "Inherited Legal Systems and Effective Rule of Law: Africa and the Colonial Legacy," 39 J. Mod. Afr. Stud. 571, 576 (2001).

⁴⁶ Anghie Antony, *Imperialism, Sovereignty, and the making of International Law*, Cambridge studies in International and Comparative Law (Cambridge, England: 1996) (Cambridge, UK; New York: Cambridge University Press, 2005).

disproportionately benefit from a system that discriminates against African nations, whereby local privacy needs are often overlooked.

In parallel, TWAIL emphasizes the significance of context-sensitive analysis in addressing Africa's diverse data governance and privacy protection needs. It promotes inclusive, bottom-up approaches where local communities, civil society organizations, and stakeholders collaborate in designing both data protection and privacy laws and policies. This acknowledgment of Africa's diversity tailors approaches to developing regulatory frameworks that strike a balance between the protection of privacy rights, the ethical use of data, digital innovation, and the promotion of social and economic development.

1.6 Contextualizing privacy and data protection

In the subsequent chapters, I explore the Afrocentric perspective on privacy and data protection, particularly emphasizing the inherent differences between African and Western societies. South African philosopher, B. J. van der Walt aptly points out that investigating these perspectives offers valuable insights into the ontological, anthropological, epistemological, and axiological distinctions between these cultural contexts.⁴⁷ While African societies are far from homogeneous, this thesis draws primarily on shared philosophical principles, such as communalism, that remain prevalent across many African traditions and continue to shape conceptions of privacy and personhood. While the comprehensive exploration of these differences awaits detailed discussion in later chapters, it is essential to highlight their significance in shaping views on privacy and data protection.

Within the African cultural context, communalism and the interconnectedness of individuals within the community stand as central themes.⁴⁸ Specifically, African ontology

⁴⁷ Van Der Walt, B.J. 1997. Afrocentric or Eurocentric: our task in multicultural South Africa. Potchefstroom University for CHE.

⁴⁸ Adeshina Afolayan, Individualism, Communitarianism and African Philosophy: A Review Essay on Exploring the Ethics of Individualism and Communitarianism, <https://news.clas.ufl.edu/individualism->

stresses the notion of belonging to and actively participating in collective activities, beliefs, rituals, and festivals of the community.⁴⁹ In this view, human identity is intricately tied to the collective identity, with individual actions and thoughts harmoniously aligned with those of the community.⁵⁰ In contrast, the Western worldview places a greater emphasis on individuality and self-reliance, whereby the individual is perceived as meaningful in their own right and not solely dependent on the community for their sense of identity or existence.⁵¹ Furthermore, the African cultural perspective highlights the transcendental nature of the collective “we,” which is inseparable from its individual components. The self is viewed as indivisible from the community, and individual identity is deeply influenced by social interactions and communal life.⁵² Conversely, the Western notion of “community” often revolves around self-interested individuals, with individual rights taking precedence over communal duties.⁵³

Similarly, ethics in African societies prioritize fulfilling duties to the community over asserting individual rights. In particular, each member of the community bears a moral responsibility to contribute to the overall well-being, and the rule of law aims to restore social harmony rather than merely protect individual rights.⁵⁴ Moreover, moral personhood in the African context is intricately linked to how the community shapes and educates individuals, with moral principles practically applied in daily life to promote human well-being and

[communitarianism-and-african-philosophy-a-review-essay-on-exploring-the-ethics-of-individualism-and-communitarianism/](#).

⁴⁹ *Ibid.*

⁵⁰ Ibrahim Anoba, A Libertarian Thought on Individualism and African Morality, <https://www.africanliberty.org/2017/05/21/a-libertarian-thought-on-individualism-and-african-morality-by-ibrahim-anoba/>.

⁵¹ James Q. Whitman, The Two Western Cultures of Privacy: Dignity Versus Liberty <https://www.yalelawjournal.org/article/the-two-western-cultures-of-privacy-dignity-versus-liberty>.

⁵² Menkiti, Ifeanyi A. 1984. "Person and Community in African Traditional Thought." In African Philosophy: An Introduction, edited by Richard A. Wright, 171–81. New York: University Press of America.

⁵³ *Ibid.*

⁵⁴ Ikuenobe, Polycarp. 2006. Philosophical Perspectives on Communalism and Morality in African Traditions. Lanham: Lexington Books.

communal existence.⁵⁵ Consequently, traditional African cultures connect an individual's identity deeply to the virtues, values, and beliefs instilled by the community, reflected in their actions and decisions.⁵⁶

With this foundation, throughout this thesis, I scrutinize the emphasis on communal spirit, interconnectedness, and shared responsibility within African communities. I explore how individual identity is profoundly intertwined with the collective and how moral principles prioritize the well-being of the community. Understanding and respecting these cultural values are crucial when considering privacy and data protection in an African context, where community welfare holds high regard. In the subsequent chapters, a detailed examination unfolds, elucidating how these Afrocentric perspectives can influence privacy practices and data protection policies in contemporary African societies.

1.7 Problem Statement

In the face of the rapid surge in internet usage across Africa, significant progress has been made in the continent's digital environment. While these advancements hold potential for further expansion and development, concerns have emerged regarding the adequacy of existing privacy and data protection laws to address the unique challenges faced in Africa. Many African nations have embraced the European Union's GDPR framework to tackle these issues. However, the widespread adoption of the GDPR as a model for privacy and data protection in Africa raises questions about its relevance within African cultural contexts and its ability to effectively address privacy concerns in Africa.

Consequently, three primary challenges come to the forefront. First, there is the issue of cultural compatibility. The GDPR, while internationally accepted, is built on Western principles, which could lead to conflicts with African cultural values, traditions, and legal

⁵⁵ *Ibid.*

⁵⁶ *Ibid.*

structures. The second issue relates to corporate influence. Critics argue that the provisions of the GDPR might disproportionately benefit large corporations at the expense of individual African citizens. The last deals with developmental disparities. The prevailing uniformity of the GDPR might not adequately account for the varying stages of development seen across different African countries. Hence, a more refined and adaptable approach is needed to probe into both collective and individual data protection rights effectively in Africa's diverse context. Accordingly, the subsequent chapters analyze these challenges and propose nuanced solutions that consider Africa's unique cultural and developmental context.

1.8 Purpose of the Study

This research investigates the implications and challenges of adopting and implementing privacy and data protection regulations, specifically the GDPR, in the African context. To this end, the research uses the TWAIL perspective to inform development with an appropriate regulatory framework concerning privacy and data protection.

1.9 Specific Research Objectives

This research aims to achieve the following specific objectives:

- 1) To examine the limitations and challenges of implementing the European GDPR to establish comprehensive privacy and data protection laws in Africa.
- 2) To investigate the existing mechanisms, frameworks, and initiatives within Africa to address privacy and data protection laws.
- 3) To assess how privacy and data protection regulations in Africa can be tailored to the region's unique cultural, social, and economic factors.

1.10 Research Questions

The overarching question addressed by this thesis is:

What are the implications and challenges of adopting and implementing the GDPR, in the African context, and how can the TWAIL perspectives inform the development of a contextually appropriate regulatory framework?

To address this overarching question, the thesis explores the following sub-questions:

- I. What are the challenges and limitations of implementing the GDPR to establish comprehensive privacy and data protection laws in Africa?
- II. What existing mechanisms, frameworks, and initiatives are already in place within Africa to address privacy and data protection laws?
- III. How can privacy and data protection regulations in Africa be tailored to the region's unique cultural, social, and economic factors?

1.11 Thesis Statement

Adopting the GDPR as a model for privacy and data protection legislation in Africa presents opportunities and challenges. While the GDPR offers a comprehensive framework, its applicability in Africa raises concerns regarding cultural compatibility, corporate influence and developmental disparities. Therefore, a contextually tailored approach to privacy and data protection regulation in Africa is necessary, one that accounts for the continent's diverse cultural values, power imbalances, and varying levels of socio-economic development.

1.12 Thesis Argument

The main argument of the thesis is that privacy and data protection regulations in Africa need to be tailored to accommodate the diverse cultural context and local traditions. In particular, within the African cultural framework, the importance of communal living and the interconnectedness among individuals within the community stand out. Specifically, the concept of African ontology emphasizes the significance of belonging and active engagement

in the collective activities, beliefs, rituals, and celebrations of the community.⁵⁷ In this way, personal identity in the African context is closely intertwined with the identity of the community, resulting in a seamless alignment between individual actions and the values of the community.⁵⁸ In contrast, the Western viewpoint places a stronger emphasis on individualism and self-sufficiency.⁵⁹ Here, the Western individual is seen as having inherent value independently and is not solely reliant on the community for their sense of identity or existence.⁶⁰ Furthermore, ethical principles in African societies prioritize the fulfillment of communal duties over asserting individual rights.⁶¹ Thus, each community member bears a moral obligation to contribute to the overall well-being of the collective, where the legal system is designed to reinstate social harmony rather than just safeguarding individual rights.⁶² Consequently, adopting a uniform approach could impose Western ideas and overlook African societies' distinctive viewpoints and values.

1.13 Why Africa as one bloc?

This thesis adopts a holistic approach by considering Africa as a single entity, representing African countries' collective vision and aspirations within the African Union. The choice to contextualize Africa as a single bloc is driven by the recognition of common challenges and the importance of continental collaborations and protection, given the limited impact of individual national laws. In this context, the African Union serves as a platform for promoting economic integration, intra-African trade, and sustainable development.⁶³

⁵⁷ Etta, Emmanuel E, Dingba Dingba Esowe & Offiong O Asukwo, "African communalism and globalization" (2016) 10:3 African Research Review 302, online: <http://dx.doi.org/10.4314/afrr.v10i3.20>.

⁵⁸ M'Baye, Babacar & Polycarp Ikuenobe, "Philosophical Perspectives on Communalism and Morality in African Traditions" (2007) 41:4 African American Review 807, online: <http://dx.doi.org/10.2307/25426992>.

⁵⁹ Nnaemeka, Johnkingsley, "A Critical Discourse on African Communalism Vis-a-Vis Western Individualism: The Existential Realities" (2023) SSRN Electronic Journal, online: <http://dx.doi.org/10.2139/ssrn.4424478>.

⁶⁰ *Ibid.*

⁶¹ Ikuenobe, Polycarp, "Priority of duties, substantive human rights, and African communalism" (2021) 40:4 South African Journal of Philosophy 421–435, online: <http://dx.doi.org/10.1080/02580136.2021.2010174>.

⁶² *Ibid.*

⁶³ "Deepening African integration: Intra-African Trade for Development and Poverty Reduction" (2016) African Perspectives on Trade and the WTO 11.

Accordingly, this research acknowledges the shared goal of overcoming historical economic fragmentation and fostering regional cooperation by treating Africa as a unified bloc. It recognizes that through pooling resources, removing trade barriers, and strengthening economic ties, it is anticipated that African countries can collectively address common challenges, leverage their strengths, and achieve sustainable development on a continental scale.⁶⁴

While Africa is not a homogeneous continent, the research acknowledges common societal characteristics, particularly the prevalent communal culture shared among many African societies south of the Sahara. It also seeks to explore whether non-individualistic cultures, such as African and Asian cultures, provide space for individuals to advance privacy claims. Despite treating Africa as a whole, it is essential to note that the research also acknowledges individual African countries' diversity and unique circumstances. This balanced approach ensures that privacy and data protection regulations consider each country's specific needs and contexts, aiming to benefit all nations within the African continent.

Adopting a bloc approach to researching privacy and data protection in Africa has several advantages. Firstly, many African countries have implemented similar legal frameworks and policies regarding privacy and data protection, often influenced by international standards such as the GDPR.⁶⁵ This research can identify common patterns, challenges, and practical strategies across the region by studying Africa as a collective bloc. In addition, it can uncover similarities, gaps, and insights about the regional landscape by bringing out the common implementation challenges of privacy and data protection laws and policies across different African countries. Ultimately, this approach helps to understand the strengths and weaknesses of different privacy and data protection frameworks, thereby

⁶⁴ *Ibid.*

⁶⁵ Alex B. Makulilo, *supra* note 33.

leading to informed recommendations. Moreover, considering Africa as one bloc improves data accessibility, thus overcoming data limitations and gaining a more comprehensive understanding of the state of privacy and data protection in Africa.

Treating Africa as a single bloc also enables the formulation of regional policy recommendations. In this way, the research findings can inform regional initiatives, collaborations, and advocacy efforts to strengthen African privacy and data protection. Consequently, this approach allows for more impactful policy interventions that address regional challenges and promote harmonization of privacy laws and standards.

Furthermore, considering Africa as one bloc acknowledges the importance of a pan-African perspective. It recognizes African countries' interconnectedness and shared interests in addressing privacy and data protection challenges in the digital era.⁶⁶ This broader understanding of regional dynamics enables collaborative efforts to protect individual rights and fosters a culture of data privacy in Africa.

However, treating Africa as a single bloc is not without its limitations. This approach risks overlooking important variations in legal capacity, institutional development, and socio-political realities across individual countries. It may also obscure the specific needs of smaller or less-represented states, whose perspectives can be diluted within a continent-wide framework. A bloc perspective can also oversimplify complex intra-regional differences, potentially resulting in generalized policy recommendations that may lack relevance or effectiveness at the national level. To address these concerns, this research adopts a balanced approach, one that identifies regional trends and commonalities while remaining sensitive to the legal, cultural, and developmental diversity that characterizes African countries.

1.14 Methodology

⁶⁶ Deepening African integration: Intra-African Trade for Development and Poverty Reduction. (2016). *African Perspectives on Trade and the WTO*, 11–11. doi:10.30875/e5b1e7e1-en.

This thesis utilizes a legal doctrinal approach that goes beyond simplified doctrinal logic to address the research questions extensively. Notably, the doctrinal method has been widely used in previous studies to examine reform processes, assess the effectiveness of existing laws, and develop new legal principles. Its primary objective, therefore, is to enhance the significant aspects of the law and contribute to legal development. Therefore, this thesis utilizes doctrinal legal analysis to trace the evolution and interpret privacy and data protection legislation in Africa and Europe.

In terms of analysis, the approach of this thesis is qualitative, focusing on the analysis of the GDPR and its applicability to African states within the context of the African Union. Specifically, doctrinal legal research is employed to examine the history, objectives, and development of the GDPR. This approach aims to systematically expose the privacy and data protection laws and regulations in Africa and to explore the relationship between European Union data protection regulations, particularly the GDPR, and various African privacy and data protection rules, including the AU Convention and regional instruments. Through this analysis, key areas of difficulty can be identified, enabling potential future developments to be predicted.

Moreover, a logical examination of the law characterizes the doctrinal legal methodology through legal reasoning. It involves locating and interpreting the sources of law, which in this case include texts related to privacy and data protection, European law, and relevant legal doctrines and principles. By adopting this methodology, the thesis aims to evaluate privacy and data protection legal frameworks in international, European, and African contexts. This evaluation assists in identifying suitable regulatory approaches in Africa.

For the purposes of research, the thesis relies on existing literature and relevant documents, such as activity reports, member participation information, and extension process projects of the GDPR to African states from the Council of Europe website. Additionally,

documents from European and African regulatory offices, including statements made during meetings, written reports, and projects that support integrated concepts from both contexts, are also reviewed. Furthermore, the African Union website is a valuable resource for progress reports on the AU Convention and provides insights into African states' perspectives on privacy and data protection regulation within the African Union. Given the doctrinal orientation of this research, the analysis draws primarily on secondary sources rather than empirical fieldwork. While national case studies would provide additional empirical grounding, they fall outside the current scope and are identified as a priority for subsequent work.

Ultimately, this methodology aims to comprehensively understand the legal regimes governing privacy and data protection, thereby facilitating comparisons between European and African approaches and informing effective regulation in the African context.

1.15 Significance, Justification, and Scope of the Study

First and foremost, the thesis addresses an understanding gap surrounding privacy and data protection regulations in Africa. This gap refers to the limited comprehension of how privacy and data protection frameworks, many of which are based on Western models, fail to account for Africa's unique socio-cultural, legal, and economic contexts. For clarity, references in this thesis to Western approaches primarily denote the European Union's data-protection tradition. In particular, current discourse and regulatory frameworks often overlook the specific needs, values, and practices prevalent across African countries, especially the communal nature of privacy and data sharing in African societies. By examining the shortcomings of existing regulations and highlighting the importance of culturally relevant frameworks, this thesis contributes to a more nuanced understanding of privacy and data protection that is both effective and contextually appropriate for Africa.

Although data protection and privacy laws have rapidly evolved globally, they still need to adequately address African countries' specific needs and challenges. By exploring the implications of GDPR within Africa's unique cultural, social, and economic factors, this research advances the understanding of how privacy and data protection regulations may be tailored specifically for Africa's context.

Furthermore, this thesis provides policymakers and regulatory bodies in Africa with invaluable insight. By exploring the challenges associated with implementing the GDPR in addition to existing mechanisms and initiatives in their region, policymakers gain access to valuable information and resources for making informed decisions on developing privacy and data protection laws that are practical, contextually relevant, and aligned with African values and needs. In turn, it can help formulate policies that promote innovation while safeguarding culturally sensitive privacy rights and simultaneously encouraging economic development through digital channels. As a result, this thesis contributes to the academic discourse surrounding privacy, data protection and digital governance in Africa. By employing TWAIL analysis of Western legal theories in contrast to African realities, this research offers fresh insights into the governance of privacy and data protection in Africa. Furthermore, it aids a greater understanding of how global legal frameworks can be tailored more appropriately to suit developing regions for a more equitable international legal order.

Additionally, this thesis promotes inclusive digital governance. It highlights the significance of including Africa's perspective and interests in global discussions on digital norms and governance by emphasizing their needs within African societies and the potential pitfalls associated with adopting Western-centric legal frameworks without taking local context into account. By doing this, this thesis contributes to fostering more equitable digital governance, which bridges the digital divide and provides African users with privacy rights protection whilst taking full advantage of opportunities offered by the digital revolution. By

taking an African perspective into account, this thesis seeks to empower African digital users by protecting their privacy rights in an ever-evolving digital environment.

In light of this focus on inclusivity and equitable digital governance, the importance of privacy and data protection regulation has gained significant attention from the African Union and has become a global phenomenon. However, it is crucial to recognize the need for a unique regulatory approach that considers the systematic differences among regions. This recognition emphasizes determining the most suitable regulatory strategy tailored to the African context. Furthermore, the utilization of the TWAIL framework introduces a unique and comprehensive perspective to the subject matter. This approach sets it apart from prior research, enabling a deeper exploration of privacy and data protection regulations within the African context.

The literature reveals that applying European privacy and data protection regulations as it is may lead to potential gaps in the effectiveness of privacy and data protection laws in Africa. Thus, the scope of this thesis is focused on the African Union and the European Union. Specifically, it explores the subject matters of privacy and data protection laws within this context. While this thesis engages with both privacy and data protection, its primary orientation is toward data protection as the operative legal expression of privacy interests in Africa. Privacy serves here as the broader normative foundation, with data protection functioning as the regulatory instrument through which privacy is most directly shaped, enforced, and experienced on the continent. What sets this thesis apart is its concentrated examination of both Africa and the European Union, allowing for a more focused analysis.

To comprehensively understand privacy and data protection regulation in Africa, this thesis adopts TWAIL as its theoretical framework. By juxtaposing the European Data and Privacy Regulation with developments on the subject from the African bloc, it offers a distinct perspective compared to existing studies. This choice of framework facilitates a

deeper exploration of privacy and data protection regulation within the African context. Moreover, a significant aspect of this thesis is its focus on the African cultural context of privacy and data protection. This could be identified as the realm of African ontology.

Overall, this thesis stands out due to its narrowed scope, focusing on the African and European Union, its examination of privacy and data protection laws, and its adoption of the TWAIL theoretical framework. Its approach and geopolitical orientation uniquely contribute to the existing body of knowledge. Through its findings and analysis, this thesis aims to enhance the understanding of privacy and data protection regulation in Africa, thereby contributing to developing more effective regulatory approaches tailored to Africa's specific needs.

1.16 Chapter Synopsis

The present chapter introduces the thesis and provides an overview of the research topic, emphasizing the significance of privacy and data protection in Africa. The chapter outlines the research problem and the research objectives. Furthermore, it presents the structure of the thesis and discusses the methodology employed for conducting the research.

Chapter 2 lays the foundation for the research by establishing and elaborating on the theoretical framework that guides the analysis of Africa's regulatory approach to privacy and data protection. The TWAIL lens is adopted as the theoretical perspective, providing valuable insights into the unique challenges and considerations within the African context. The chapter explores the key concepts and principles of TWAIL, elucidating its relevance to the research and how it informs the examination of privacy and data protection regulations in Africa. By utilizing this framework, the thesis aims to gain a deeper understanding of the complexities and dynamics that shape privacy practices in Africa.

Chapter 2 also conducts a comprehensive literature review on privacy and data protection in Africa. It examines existing studies, scholarly works, and reports, with a specific focus on the adoption of European law, notably the GDPR, in African countries. Through this review, the thesis identifies gaps, challenges, and opportunities in implementing privacy laws within the African context, thereby contributing to a holistic understanding of privacy and data protection issues on the continent.

Chapter 3 addresses the first research question, examining the challenges and limitations of implementing the GDPR to establish comprehensive privacy and data protection laws in Africa. The chapter explores legal, cultural, technological, and institutional challenges faced by African countries in adopting and implementing the GDPR, discussing their implications on privacy and data protection regulations' effectiveness. To provide cultural insights on privacy in Africa, this thesis draws upon both anthropological and sociological sources. Anthropological perspectives are employed to examine privacy within the context of African communal traditions, social norms, and historical practices, while sociological studies contribute to understanding the impact of privacy norms on social structures and interactions in modern African societies and interactions in modern African societies.

Chapter 4 focuses on the second research question, investigating the existing mechanisms, frameworks, and initiatives in Africa to address privacy and data protection laws. The chapter critically examines the current state of privacy and data protection regulations in African countries, analyzing initiatives, policies, and legal frameworks developed by the African Union and regional organizations. It also assesses the effectiveness and limitations of these mechanisms.

Inspired by insights from the cultural anthropology of privacy in Africa, Chapter 5 examines the third research question, exploring how a contextually tailored approach to

privacy and data protection regulation can be developed and adopted in Africa, considering unique cultural, social, and economic factors. The chapter examines alternative techniques that align with the African context, emphasizing the importance of cultural norms, societal values, and economic conditions in designing effective rules. It also provides potential strategies and recommendations for developing contextually tailored privacy and data protection frameworks.

Chapter 6 summarizes the key research findings and discusses their implications, highlighting the thesis' contributions to the field of privacy and data protection in the African context. The chapter concludes by offering recommendations for policymakers, organizations, and stakeholders to enhance Africa's privacy and data protection regulations. It also identifies areas for future research and suggests potential avenues for further exploration within the field.

Chapter Two: Literature review and theoretical framework

2.1 Introduction

The first section of this chapter conducts a comprehensive literature review to explore the multifaceted domain of privacy and data protection in Africa, carefully exploring the evolving framework of privacy and data protection laws within Africa. It also illustrates the intricate interplay of cultural, legal, and technological influences. It begins with an acknowledgment of privacy's dual nature as both a personal right and a public concern, deeply embedded in the collective identity and societal well-being of African cultures. Through the pioneering efforts of scholars like Johann Neethling⁶⁷ and subsequent academics, the review probes the challenges of reconciling Western-centric privacy theories with African communal values, highlighting a notable gap in understanding privacy within these unique cultural frameworks. As the review progresses, it explores the constitutional framework across African countries, highlighting the varying degrees of privacy protection embedded within national constitutions and the broader adoption of privacy rights in legal structures. Despite this, a significant gap emerges in the translation of constitutional mandates into effective, comprehensive data privacy legislation, with some countries demonstrating robust frameworks while others lag.

In tandem, the advent of Information and Communication Technologies (ICTs) introduces a new dimension to the privacy discourse, amplifying concerns over personal data collection and the potential for misuse. Here, the literature identifies a critical need for

⁶⁷ Neethling, J, "The Concept of Privacy in South African Law" (2005) 122:1 *The South African Law Journal* 18–28.

sophisticated legal and regulatory frameworks that navigate the complexities introduced by digital advancements, pointing to a gradual legislative response across the continent. However, the review emphasizes a persistent gap in the enforcement and practical application of these laws, alongside the challenges of integrating European standards and indigenous cultural practices into cohesive privacy protections. Furthermore, the review briefly touches upon the role of religion, particularly Islam, due to its prominent role in shaping legal systems in several African countries, especially in North and West Africa. This exploration highlights the diversity of approaches to integrating religious principles with modern privacy and data protection mandates. This acknowledgment further emphasizes the complexity of formulating privacy protections that resonate with the continent's multifaceted cultural and religious identities.

One of the most notable gaps identified in the literature is a comprehensive understanding of privacy and data protection from an indigenous African perspective. Despite efforts to compare Western and African views on privacy, there exists a marked deficiency in deeply exploring how privacy is conceptualized, valued, and protected across different African cultures, legal systems, and socio-technological contexts. This gap calls for more detailed, context-specific research that moves beyond the contrast of Western individualism and African communalism, aiming to uncover a nuanced understanding of privacy that aligns with the continent's diverse cultural traditions and legal frameworks. In essence, this literature review sets the stage for addressing the multifaceted nature of privacy and data protection in Africa, highlighting significant legislative progress while also revealing critical gaps in research, implementation, and the harmonization of global standards with local realities. It calls for a concerted effort to bridge these gaps, advocating for a holistic approach that respects the unique socio-cultural and legal nuances of African societies in the digital age.

Section two of this chapter introduces the theoretical background of the analysis using TWAIL. The discussion is split into four main sections for clarity. The first section looks at historical influences, examining the impact of colonial legacies and power imbalances on legal systems and how they affect privacy and data protection standards in Africa. It seeks to show how colonialism continues to influence current legal practices and privacy standards, drawing links between historical and contemporary challenges in regulatory and power structures. The second section tackles the critique of Eurocentrism, a crucial aspect of TWAIL. This part critically examines the effects of Eurocentric views on the conversation around privacy and data protection in Africa, shaping how these matters are viewed and addressed. It highlights the need to rethink these influences to create a more inclusive and fair approach to legal standards across the continent. In the third section, the focus shifts to the idea of dependency, another important concept in TWAIL. This discussion highlights how global legal imbalances affect Africa's regulatory framework, exploring how international legal structures contribute to dependencies that challenge the creation of just and effective privacy and data protection strategies in African settings. Lastly, the fourth section discusses Human Rights and Social Justice within the TWAIL framework. While not the primary focus, this topic is essential for grasping the wider effects of privacy and data protection laws in Africa. It emphasizes the importance of taking into account Africa's distinct historical, social, and cultural contexts when developing and applying these laws, advocating for an approach to rights that acknowledges the unique aspects of African societies. Collectively, these sections lay out the theoretical groundwork for the analysis, providing important perspectives on the complexities of privacy and data protection in the African context.

2.2 Literature review

“...privacy is not just a personal matter but also a public good that affects collective identity and well-being.”⁶⁸

The conceptualization of privacy and data protection in the African cultural context has been a relatively understudied area in existing literature. While a few authors have ventured into this realm, there remains a significant gap in comprehensively addressing the complexities and nuances of privacy within African cultures, which often emphasize communal values, collective rights, and intricate social relationships. Neethling⁶⁹ stands as one of the pioneering authors who have attempted to define privacy within the African context, despite the emergence of many subsequent authors who have tried to clarify and define privacy with no clear consensus or conclusion. While Neethling’s contributions are commendable, his work tends to rely on Western perspectives of privacy, especially the control theory.⁷⁰ The control theory emphasizes individual control over personal information and autonomy, principles that have greatly influenced privacy discourse globally.⁷¹ The challenge in applying Western-centric privacy theories to the African context lies in the fundamental differences in cultural values. African societies often emphasize communal values, prioritizing collective rights and the importance of social relationships, a stark contrast to Western individualism.⁷² This discrepancy leads to a significant gap, as Western perspectives may not fully recognize the unique cultural norms, practices, and legal structures integral to the African understanding of privacy. While contemporary discourse often treats data protection as the primary legal mechanism for safeguarding privacy, it is important to recognize that African understandings of privacy long pre-date modern regulatory

⁶⁸ A B Makulilo, “Privacy Values in African Societies” (2016) 8:2 *Journal of Privacy Studies* 193 at 195.

⁶⁹ J Neethling, *Die Reg op Privaatheid* (LLD Thesis, University of South Africa, 1976).

⁷⁰ South African Law Reform Commission, Privacy and Data Protection Project 124 (Project Leader: J Neethling, 2001).

⁷¹ Makulilo, A.B., *African Data Privacy Laws*. Law, Governance and Technology Series 33. Springer International Publishing AG, 2016 at 198.

⁷² Makulilo, A.B., "A Person Is a Person through Other Persons—A Critical Analysis of Privacy and Culture in Africa." (2016) 7 *Beijing Law Review* 192-204.

frameworks and are rooted in communal ethics, relational identity, and culturally grounded norms of personhood and dignity.

Iain Currie's constitutional perspective takes a different approach by examining the concept of privacy in the context of the South African Constitution. Currie's research highlights the role of constitutional principles and legal frameworks in shaping privacy rights in South Africa,⁷³ noting the inclusion of privacy within specific African constitutions. Although focused primarily on South Africa, Currie's study illustrates the broader adoption of privacy rights in various African constitutions. This approach emphasizes the critical role of constitutional provisions in establishing privacy norms and protections in individual African countries. Despite existing scholarship on privacy and data protection, there is a significant gap in understanding how constitutional privacy rights interact with cultural orientations to privacy within African societies. This issue is particularly relevant in regions where customary law coexists with formal legal systems. The interplay between privacy as a constitutional right and the communal-based understanding of privacy, rooted in African customary contexts, remains largely unexplored. Investigating how these two dimensions interface is crucial for gaining deeper insights into the ways privacy rights are both conceptualized and practiced across diverse African legal frameworks. This gap in the literature draws attention to the importance of examining how constitutional law and customary privacy norms converge and diverge in shaping privacy rights in African countries. The distinct cultural, historical, and legal contexts of African societies further highlight the need for a more nuanced approach that moves beyond Western-centric models of privacy. This need becomes even more pronounced when considering the evolving perspectives on privacy across the continent, especially the complex relationship between constitutional frameworks and deeply ingrained customary norms.

⁷³ Currie, I., "The concept of privacy in the South African constitution: reprise: aantekeninge" (2008) 2008:3 *Journal of South African Law/Tydskrif vir die Suid-Afrikaanse Reg* 549-557.

2.2.1. Evolving Perspectives on Privacy in the African Context

The prolonged perception that privacy held minimal value in Africa originated from the misconception that the communal and collectivist nature prevalent in most traditional African communities during the pre-colonial era implied a lack of privacy. This viewpoint suggested that individuals could not lead independent lives without community consent.⁷⁴ In numerous traditional African societies, individualism was perceived as conflicting with established social norms, tying an individual's identity intricately to the community's identity.⁷⁵ This interpretation significantly shaped the understanding of privacy, minimizing its role in early discussions on privacy and data protection and contributing to the establishment of the dominant discourse about Africa, influencing contemporary perceptions. Contrary to this perspective, Makulilo challenges the assumption that privacy is undervalued in Africa due to its collectivist culture. According to him, "...privacy is not just a personal matter but also a public good that affects collective identity and well-being."⁷⁶ This reconceptualization recognizes privacy as both a personal and public concern, integral to collective identity and well-being. The African principle of *ubuntu*,⁷⁷ emphasizing humanity through interdependence, further highlights the relational aspect of privacy, challenging Western ideas of individual autonomy. Makulilo's analysis provides valuable insights into African society, challenging the traditional Western emphasis on individual autonomy.

⁷⁴ Makulilo, supra note 68.

⁷⁵ *Ibid.*

⁷⁶ Makulilo, supra note 68 at 195.

⁷⁷ *Ubuntu*, a central concept in African philosophy, has been interpreted variously by scholars, including figures such as Archbishop Desmond Tutu, Louw, Mokgoro, and Mbigi. At its core, Ubuntu champions a collectivist approach to human relationships and mutual aid in daily life, positing the individual's identity and well-being as deeply embedded within the community's fabric. This philosophy, which prioritizes communal considerations over individual ambitions, is particularly prominent in South African scholarship but also resonates across various African societies, reflecting a widespread cultural ethos that values interconnectedness and collective well-being.

In his analysis, Bygrave points out that African cultures often place a higher value on the community's interests rather than those of the individual.⁷⁸ He illustrates this priority by observing that the lack of specific privacy laws in many African regions is indicative of a broader cultural emphasis on the collective good. Bygrave encapsulates this idea by mentioning, "...the absence of privacy legislation in Africa reflects the priority of communal considerations over individual interests."⁷⁹ This view contrasts with the typical Western focus on safeguarding individual rights. In his 2004 study, "*Privacy Protection in a Global Context—A Comparative Overview*,"⁸⁰ Bygrave initially questioned whether societies grounded in communal values could effectively support individual privacy claims. Yet, he acknowledges a recent shift in some African nations towards embracing privacy, driven by their unique historical contexts and a cautious attitude toward the sharing of personal data.⁸¹ This change points to an increasing recognition of privacy's importance alongside communal values. The lack of clarity about the specific nature of privacy in Africa may be attributed to the predominant method of knowledge transfer within communities during the pre-colonial era. Oral traditions played a pivotal role as the primary conduit for disseminating information and communal norms.⁸² Within the rich tapestry of traditional African societies, the conveyance of knowledge and cultural values was primarily oral, utilizing a vibrant array of proverbs, songs, folktales, and narratives.⁸³ This oral tradition served as a pivotal medium for imparting generational wisdom, encapsulating critical cultural dimensions, including nuanced understandings of privacy.

⁷⁸ Bygrave, Lee A., "Privacy Protection in a Global Context—A Comparative Overview" (2004) 47 *Scandinavian Studies in Law* 319-348 at 328.

⁷⁹ *Ibid.*

⁸⁰ *Ibid.*

⁸¹ Bygrave, Lee A. *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press, 2014.

⁸² Zimu-Biyela, Acquinatta N., "Taking Stock of Oral History Archives in a Village in KwaZulu-Natal Province, South Africa: Are Preservation and Publishing Feasible?" *SciELO*. Accessed January 20, 2024. http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S0259-94222022000300013&lng=en&nrm=iso.

⁸³ *Ibid.*

The Kikuyu community of East Africa, for instance, articulates the value of privacy in domestic spheres through the proverb: “*Cia mucii ti como/cia mucii itiumaga ndira/cira wa mucii ndumagirio kiharo/ndukamenyithie wa itara*,”⁸⁴ (home affairs cannot be told to the public), eloquently urging the protection of home affairs from the public gaze. This proverb finds resonance across diverse African cultures, signifying a widespread cultural ethos that venerates privacy. Furthermore, the Rwandan saying that “*pregnancy and fire cannot be kept a secret*”⁸⁵ eloquently captures the inevitability of certain truths emerging into the public domain, offering a nuanced reflection on the bounds of privacy. In a similar vein, the pan-African proverb “*Umntu ngumuntu ngabantu*” (Zulu), translating to “*A person is a person through other persons; one cannot exist in isolation but thrives through relationships*,” profoundly emphasizes the foundational role of community and interconnectedness in African societal structures.⁸⁶ This cultural philosophy emphasizes that individuals thrive through relationships, thus reflecting the intricate balance between privacy and community. In African societies, privacy is not viewed as antithetical to communal life but is understood within a delicate balance between the public and private spheres. This balance acknowledges the importance of safeguarding personal matters while also recognizing the collective responsibility inherent in social relationships. These proverbs illustrate how African cultural orientations uphold privacy as both a personal and communal matter, reflecting a philosophical and practical alignment between privacy and interconnectedness.

The above-mentioned proverbs reveal a complex balance between privacy and community that is central to African cultural paradigms. The oral nature of these traditions, however, presents substantial challenges for the archival and systematic documentation of

⁸⁴ Africanmanners, "Gikuyu Proverbs," *African Manners*, July 7, 2012, <https://africanmanners.wordpress.com/2012/07/07/gikuyu-proverbs-1000-in-total/>.

⁸⁵ Ukwendu, Jeanne Egboisiuba, "AFRICAN PROVERBS ON PREGNANCY AND BIRTH," *Bella Online, The Voice of Women*. Accessed January 26, 2024, <https://www.bellaonline.com/articles/art69184.asp>.

⁸⁶ Olinger, Hanno N., Johannes J. Britz & Martin S. Olivier, "Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa" (2007) 39:1 *The International Information & Library Review* 31-43.

privacy practices, potentially hindering the development of a detailed historical narrative on the evolution of privacy across the continent. Despite the presence of individualistic elements within Africa's social structure, the prevalence of communal living often concealed notions of individualism from external observers, leading to the misconception that privacy was of marginal importance in pre-colonial Africa.⁸⁷ The advent of colonialism further entrenched these views, albeit through different mechanisms, significantly altering the indigenous development of privacy concepts on the continent.⁸⁸

Cultural and societal factors such as communal living, oral traditions, colonial legacies, and external influences play a crucial role in shaping perceptions of privacy in Africa. Gutwirth⁸⁹ suggests that in sub-Saharan Africa, the individual's interests are often seen as secondary to those of the group, which diminishes the scope for privacy. This perspective is evidenced by the absence of explicit references to privacy in the African Charter on Human and Peoples' Rights (ACHPR) of 1981, indicating a historical overlooking of privacy culture in Africa.⁹⁰ Moreover, the dominance of Western scholars in privacy discourse has led to a conceptualization of privacy that is largely framed within Western cultural norms.⁹¹ Amidst the endeavour to integrate indigenous insights into privacy and data protection frameworks, acknowledging the communal and cultural contexts, the academic discourse on privacy in Africa encounters a discernible gap, particularly in the profound exploration of Indigenous African perspectives on privacy. This gap highlights a critical oversight. While there have been efforts to compare Western and African views on privacy, there is a notable deficiency in examining the depth and nuances of privacy as conceptualized within traditional African societies. Although this thesis highlights this issue and advocates

⁸⁷ Zimu-Biyela, *supra* note 82.

⁸⁸ Reid, Richard, "How Colonialism Preempted Modernity in Africa" (2011) 39:3 *The Journal of Imperial and Commonwealth History* 536-538.

⁸⁹ Gutwirth, S., *Privacy and the Information Age*. Lanham/Boulder/New York/Oxford: Rowman & Littlefield Publishers, Inc., 2002 at 24-29.

⁹⁰ *Ibid.*

⁹¹ Makulilo, *supra* note 71 at 199.

for a culturally contextualized understanding of privacy and data protection, it is important to note that an exhaustive examination of Indigenous African privacy perspectives is beyond the scope of this thesis.

2.2.2 Definition of Privacy in Africa

To navigate this complex terrain, it is essential to bridge the gap between broad academic and theoretical discussions on privacy and their application within specific African legal frameworks. Such a bridge is crucial for translating theoretical principles on autonomy, self-determination, and the management of personal information, principles put forth by scholars such as Westin⁹² into the concrete realities of legal practice. The journey from abstract concepts of privacy, championed by figures like Warren⁹³, Brandeis⁹⁴, and Gavison⁹⁵, who advocate for non-interference, solitude, and controlled access to personal information, to their embodiment in legal frameworks is vividly illustrated in the South African legal framework through the works of Currie⁹⁶ and Neethling.⁹⁷ This transition marks a significant evolution in the understanding of privacy, from its philosophical underpinnings to its practical legal applications, showcasing the nuanced debates and interpretations that seek to balance individual privacy rights with the societal, cultural, and legal constructs that inform these rights within the African context. This connection not only highlights the complexity of privacy as a concept that transcends simplistic definitions but also showcases the dynamic interplay between global theoretical perspectives and their localization within specific legal systems, particularly within the African context, where socio-cultural norms significantly influence the understanding and enactment of privacy rights.

⁹² Westin, Alan F., "Privacy And Freedom" (1968) 25 *Wash. & Lee L. Rev.* 166.

⁹³ Warren, Samuel D. & Louis D. Brandeis, "The Right to Privacy" (1890) 4:5 *Harvard Law Review* 193-220.

⁹⁴ *Ibid.*

⁹⁵ Gavison, Ruth, "Privacy and the Limits of Law" (1980) 89:3 *The Yale Law Journal* 421-471.

⁹⁶ Neethling, *supra* note 67 at 22.

⁹⁷ Currie, *supra* note 73 at 552.

In exploring the concept of privacy within the African context, a sophisticated dialogue emerges that intricately blends the established legal structures with the continent's diverse socio-cultural values and scholarly debate. Privacy's legal architecture, deeply rooted in constitutional and human rights protections, acts as a formidable defence against undue invasions, signalling society's formal recognition of the significance of privacy.⁹⁸ This legal acknowledgement is seamlessly interwoven with the socio-cultural facets of privacy, embracing a more expansive understanding that Westin profoundly describes as affording "*a time for self-evaluation and for protected communication.*"⁹⁹ Privacy, therefore, is not a static concept but one deeply embedded in the structures of societal norms and cultural expectations, highlighting its dynamic and context-sensitive nature amid the varied cultural contexts of Africa.

The quest within academia to precisely define privacy reveals a consistent challenge: the elusive consensus on its definition is reflective of the concept's intricate nature. Scholars strive to balance the traditional quest for solitude with the modern need for control over personal information in an age where digital technologies continue to disrupt conventional boundaries. Bygrave aptly notes that the "*vagueness of the privacy concept*" serves a dual purpose: it accommodates a spectrum of concerns arising from ever-more pervasive data-processing activities, yet this same vagueness can hinder a clear understanding.¹⁰⁰ The complex socio-political nature and the rich cultural heterogeneity of Africa pose unique hurdles in formulating a singular, all-encompassing definition of privacy. The continent's collective culture, in contrast with the Western idea of privacy as an individualistic pursuit, highlights the profound cultural differences that shape perceptions of privacy.¹⁰¹ Gutwirth's blunt observation that privacy may hold minimal significance when viewed through a pan-

⁹⁸ Westin, *supra* note 92.

⁹⁹ *Ibid.*

¹⁰⁰ Bygrave, *supra* note 78; Bygrave, *supra* note 81 at 328.

¹⁰¹ Makulilo, *supra* note 71.

sub-Saharan lens casts a spotlight on the varying importance ascribed to privacy across different cultural contexts, elucidating the delicate interplay between communal norms and the adoption of global privacy standards.¹⁰²

Understanding privacy in Africa requires navigating a complex web of legal protections, socio-cultural interpretations, and academic debates. The synthesis of insights from scholars like Westin¹⁰³, who explores the broad roles of privacy, Bygrave¹⁰⁴, who explores the digitalization challenges, and Gutwirth¹⁰⁵, who examines cultural differences, provides a comprehensive perspective. This collective understanding not only highlights the difficulties of defining privacy in a constantly evolving digital landscape but also underlines the importance of adopting an approach that respects the rich and dynamic socio-cultural context of Africa.

2.2.3 Culture, privacy, and data protection

Building on the above argument, the discussion on culture, privacy, and data protection in Africa takes a significant step forward by examining the cultural foundations that set African societies apart from their Western counterparts. Although existing literature may not focus exclusively on the impact of culture on privacy norms within Africa, it sheds light on communal values and behaviours that play a crucial role in shaping these norms. African societies, known for their strong communal orientation, offer a contrasting view to the individualistic focus on privacy found in Western cultures.¹⁰⁶ This difference is evident in various aspects of life, including living arrangements and social responsibilities, which profoundly impact perceptions of privacy. For example, it is common in many African

¹⁰² Gutwirth, *supra* note 89.

¹⁰³ Westin, *supra* note 92.

¹⁰⁴ Bygrave, Lee A, "Privacy and Data Protection in an International Perspective" (2010) 56 *Scandinavian Studies in Law* 165-200 at 193; Bygrave, Lee A, "Data Protection Pursuant to the Right in Human Rights Treaties" (1998) 6:3 *International Journal of Law and Information Technology* 247-284 at 283; Bygrave, *supra* note 81; Bygrave, *supra* note 78 at 328.

¹⁰⁵ Gutwirth, *supra* note 89 at 24-29.

¹⁰⁶ Olinger et al., *supra* note 86.

communities for extended families to live nearby, or even under the same roof, creating a support network that naturally challenges Western concepts of personal space and suggests a collective approach to life and privacy.¹⁰⁷ Additionally, the role of rituals and communal events, crucial for social bonding and identity within African cultures, tends to blur the lines between private and public spheres, further illustrating the unique cultural approaches to privacy on the continent.¹⁰⁸

Highlighting the complexity of privacy in African contexts, Motsamai Molefe's work challenges the binary view of African ethics as purely communitarian versus the individualistic ethics of the West.¹⁰⁹ By examining concepts like personhood and dignity within African moral philosophy, Molefe presents a nuanced perspective that acknowledges individuality within the communal structure of African societies.¹¹⁰ This individuality articulated through the lens of personhood, suggests that privacy and data protection in Africa cannot be simplistically framed as antithetical to communal values but must be understood in the context of a balance between individual dignity and communal well-being.¹¹¹

Cobbah's¹¹² investigation into African values within the human rights conversation adds depth to this discussion. Cobbah highlights the communal principles of African societies, emphasizing the utmost importance of the community's survival and harmony.¹¹³ These principles, though appearing to conflict with the Western emphasis on individual rights, including privacy, present a unique lens for interpreting human dignity and rights from an Afrocentric viewpoint. The challenge, according to Cobbah, is in weaving these communal values into the worldwide conversation on privacy and data protection, which has largely

¹⁰⁷ *Ibid.*

¹⁰⁸ *Ibid.*

¹⁰⁹ Molefe, Motsamai. "Individualism in African Moral Cultures." *Cultura: International Journal of Philosophy of Culture and Axiology* 14, no. 2 (2017): 49-68.

¹¹⁰ *Ibid.*

¹¹¹ *Ibid.*

¹¹² Cobbah, Josiah A. M. "African Values and the Human Rights Debate: An African Perspective." *Human Rights Quarterly* 9, no. 3 (1987): 309-331.

¹¹³ *Ibid.*

been influenced by Western standards.¹¹⁴ The scholarly discourse highlights an evolving recognition of privacy rights within African countries, influenced by a confluence of factors including adherence to international human rights frameworks and economic considerations. Bygrave's¹¹⁵ insightful analysis sheds light on the nascent enthusiasm for privacy legislation across Africa, spurred by the imperative to align with international benchmarks, notably the EU's GDPR. This growing interest signifies a sophisticated interaction between the inherent communal orientations of African societies and the international momentum toward enhancing privacy safeguards. Within the academic discourse, it is often suggested that the conceptualization of privacy in Africa remains underdeveloped, primarily due to the collectivist environment prevalent in these societies, a sharp divergence from the individualistic inclinations of Western cultures.¹¹⁶ This communal orientation, as explored by scholars including Gutwirth,¹¹⁷ and Bygrave,¹¹⁸ is thought to diminish the agency of individuals in advocating for their privacy rights, given the overarching communal focus that characterizes life in many African settings.

The discourse surrounding privacy rights in Africa, while recognizing the shift towards their formalization, necessitates a more detailed examination to fully grasp its complexity. Bygrave's¹¹⁹ caution against viewing African cultures as monolithic and resistant to change highlights the evolving nature of privacy rights recognition within the continent. This recognition, propelled by international legal obligations, the push towards EU data protection standards, and efforts to rectify historical injustices, notably in South Africa, indicates a significant move towards integrating privacy rights within the legal systems of

¹¹⁴ *Ibid.*

¹¹⁵ Bygrave, *supra* note 104.

¹¹⁶ Makulilo, *supra* note 71.

¹¹⁷ Gutwirth, *supra* note 89.

¹¹⁸ Bygrave, *supra* note 104.

¹¹⁹ Bygrave, *supra* note 81.

African countries.¹²⁰ Such developments suggest a sophisticated evolution in African approaches to privacy and data protection, reflecting a dynamic interplay between traditional communal values and the emerging paradigm of individual privacy rights. This progression towards aligning with the global data protection paradigm, especially those standards set by the EU, highlights the complexity of navigating privacy rights within diverse African contexts. However, the literature reveals a gap in exploring the intricate ways African societies balance communal values against the backdrop of individual privacy rights, pointing towards the necessity for context-specific research. This need for in-depth studies is crucial for understanding the varied conceptualizations, valuations, and protections of privacy across different African cultures and legal frameworks.

2.2.4 Religion, Privacy, and Data Protection

Within the ambit of this thesis, while the focal point predominantly rests on the cultural and legal dimensions influencing privacy and data protection in Africa, it becomes essential to briefly touch upon the influence of religious beliefs, particularly Islam, on these discussions. This mention is crucial to highlight the complexities inherent in African nations and how religion can shape privacy practices, albeit not the central theme of this study. While this thesis does not undertake a comparative study of religious traditions, Islam is referenced in particular due to its direct integration into the legal and governance structures of several African countries. In regions such as North Africa, northern Nigeria, and parts of West Africa and the Sahel, Sharia law significantly influences statutory and customary law. This unique legal relevance explains the emphasis on Islam in scholarly and policy discussions concerning privacy in Africa. Scholarly literature often explores the complexities that arise when Islamic principles are woven into state law, highlighting both normative tensions and points of convergence. Contrasting viewpoints emerge within this discourse: on one hand,

¹²⁰ *Ibid.*

concerns are raised about the potential dilution of privacy rights through the fusion of religious doctrines and state operations; on the other hand, a segment of academia posits a compatible relationship between Islam and the principles of privacy, challenging the notion of inherent conflict.

The critical analyses by Mireille M. Caruana,¹²¹ Joseph A. Cannataci,¹²² and Ayo Kusamotu¹²³ exemplify the rigorous examination of privacy within Islamic settings, especially against the backdrop of international data protection norms like the EU Directive 95/46. Their investigations point to the chasm between legislative enactment and its practical enforcement, highlighting discrepancies in standards, particularly in law enforcement's handling of personal data. Kusamotu's exploration of Nigeria's legal landscape further illuminates the gap between constitutional guarantees of privacy rights and the actualization of these rights, alongside the broader challenges of aligning with European data protection standards.¹²⁴ The literature tends to overlook the dynamic between informal governance mechanisms, local customs, and everyday privacy negotiations within Muslim communities. This gap signifies a substantial area for future research to understand how traditional Islamic values are reconciled with the demands of digital modernity and global data flows. Additionally, there exists a scarcity of comparative analyses of Islamic privacy and data protection frameworks against other religious or secular systems within Africa, a research avenue that could yield insights into the unique facets of Islamic practices affecting privacy protections.

¹²¹ Caruana, MM, & Cannataci, JA. "European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States." *Information & Communications Technology Law* 16, no. 2 (2007): 99-124.

¹²² *Ibid.*

¹²³ Kusamotu, A. "Privacy Law and Technology in Nigeria: The Legal Framework Will Not Meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/46." *Information & Communications Technology Law* 16, no. 2 (2007): 149-159.

¹²⁴ *Ibid.*

Lastly, the prevailing scholarship often portrays Islamic practices and interpretations as homogenous, neglecting the rich diversity and regional variances within Islamic jurisprudence. This misses the broad spectrum of Islamic thought and its influence on privacy and data protection, highlighting the necessity for a more differentiated approach that considers the wide array of interpretations and practices within Islam. Thus, while this thesis does not explore deeply the religious dimensions, acknowledging these aspects highlights the layered complexity of privacy and data protection issues in African contexts influenced by religious practices. This consideration sets the stage for exploring another critical dimension that intersects significantly with privacy and data protection: the realm of developmental priorities.

2.2.5 Developmental Priorities, Privacy, and Data Protection

The relationship between development goals and privacy and data protection in Africa unveils a complex story. In the post-independence era, the rush to meet immediate political, economic, and social needs has inadvertently led to the marginalization of privacy concerns. Scholars, including Ncube, argue that the urgent push to address a range of development challenges has eclipsed the equally crucial need to establish strong data protection and privacy frameworks.¹²⁵ This development-centric approach, with its keen focus on socio-economic improvement and infrastructure development, has resulted in a scenario where privacy considerations are often viewed as secondary. Ncube's analysis highlights a prevalent trend across African countries to postpone privacy and data protection issues in favour of pressing development goals.¹²⁶ This suggests that an essential recalibration is needed to ensure that development policies and the protection of individual privacy rights are not seen as mutually exclusive but are balanced effectively. Despite highlighting a significant gap in

¹²⁵ Ncube, C. "A Comparative Analysis of Zimbabwean and South African Data Protection Systems." *Journal of Information, Law & Technology* 2 (2004): 18.

¹²⁶ *Ibid.*

the literature on integrating privacy safeguards within the ambit of national development agendas, it is important to clarify that this complex interrelation between development and privacy is not the central focus of this thesis. Instead, this discussion aims to shed light on the complex nature of privacy challenges within the African setting, setting a foundational context for the subsequent exploration.

2.2.6 The Intersection of Technology, Privacy, and Data Protection in Africa

Building on the above foundation, the literature review extends its focus to the profound impact of Information and Communication Technologies (ICTs) on privacy and data protection across the African continent. This segment acknowledges the dramatic influence that the widespread adoption of ICTs has had on amplifying concerns related to personal privacy. It explores the nuanced ways in which the digital revolution has not only enabled the extensive collection of personal data but also heightened the potential for its misuse, thus intensifying the need for effective privacy safeguards. This examination further elaborates on the multifaceted nature of privacy issues in Africa, illustrating how technological advancements intersect with, and at times complicate, the pursuit of robust data protection mechanisms.

The digital era has ushered in unprecedented capabilities for gathering personal data, simultaneously raising concerns about the potential for misuse and the consequent need for enhanced privacy protections. The scholarly contributions of Banisar,¹²⁷ Manda and Backhouse,¹²⁸ Makulilo,¹²⁹ and Ncube¹³⁰ play a pivotal role in articulating the complex dynamics between the rise of ICTs and the intensification of privacy concerns within African contexts. Banisar's comprehensive analysis stands out for its exploration of the multifaceted

¹²⁷ Banisar, D. "Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information." *East African Journal of Peace & Human Rights* 16, no. 1 (2010).

¹²⁸ Manda, MI & Backhouse, J. "Addressing Trust, Security and Privacy Concerns in E-Government Integration, Interoperability and Information Sharing Through Policy: A Case of South Africa."

¹²⁹ Makulilo, *supra* note 72.

¹³⁰ Ncube, CB. "Data Protection in Zimbabwe." In *African Data Privacy Laws*, 2016, 99-116.

threats that ICTs represent to privacy. He covers a broad spectrum of concerns, from the privacy implications of various information systems to the introduction of national ID card systems, biometric passports, DNA databases, and the use of body scanners.¹³¹ Additionally, Banisar examines the impact of ICTs on communication privacy, addressing the augmented capacity for surveillance, challenges related to user identity verification, and the burgeoning issue of cybercrimes.¹³²

The discourse on the confluence of ICTs, privacy, and data protection in Africa highlights the intricate challenges posed by the advent of digital technologies. This includes not only the immediate concerns related to the collection and potential misuse of personal data but also extends to wider issues of telecommunications privacy. For instance, the enforcement of mandatory SIM card registration and the legal stipulations for the interception of communications are brought into focus.¹³³ It is important to clarify that while this discussion is crucial for understanding the broader context of privacy and data protection in Africa, it does not represent the core focus of this thesis. By highlighting the intricate challenges and the role of ICTs in shaping privacy concerns, this literature review sets the stage for a deeper exploration into the dynamic evolution of privacy and data protection laws in Africa. This transition highlights the broader context within which this research is situated, acknowledging the significant impact of technological advancements while steering the focus toward the legislative developments that have characterized the African response to privacy and data protection needs.

2.2.7 Evolution of laws on privacy and data protection in Africa

The evolution of privacy and data protection laws in Africa showcases a dynamic and multifaceted journey. African countries have adopted diverse legal mechanisms to safeguard

¹³¹ Banisar, *supra* note 127.

¹³² *Ibid.*

¹³³ Ncube *supra* note 125.

privacy, including constitutional mandates, explicit privacy rights, and comprehensive data protection legislation. The constitutional framework across the continent reveals varying approaches to privacy protection, with some countries embedding direct mandates for data protection laws, while others enshrine specific data protection principles such as access rights, purpose limitation, and sensitive data processing prohibitions.¹³⁴ This proactive legal posture highlights the significance attributed to privacy and data protection, elevating personal data protection to a fundamental right in several constitutions. Despite the absence of explicit privacy protections in some constitutions, countries like Ivory Coast and Mauritius have successfully enacted progressive data privacy laws, illustrating that constitutional silence does not preclude robust legal frameworks.¹³⁵ Conversely, countries with strong constitutional provisions for data protection, like Mozambique, have faced challenges in translating these into effective legislation.¹³⁶

The regulatory environment of data privacy laws in Africa has evolved significantly over the past two decades. Initially, Banisar's¹³⁷ 1999 assessment highlighted a glaring void, with no African country having specific data privacy laws, though South Africa was considering the Open Democracy Bill. At that time, only Uganda and Namibia were exploring freedom of information acts.¹³⁸ Gutwirth,¹³⁹ in 2002, reinforced these observations, noting the lack of privacy provisions in the African Charter on Human and Peoples' Rights (ACHR), even as some countries mentioned privacy within their constitutions. By 2004, Bygrave echoed earlier sentiments about the scarcity of comprehensive data privacy laws across the continent, with South Africa being a notable exception for including privacy rights

¹³⁴ Greenleaf, Graham, and Bertil Cottier. "International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis." *Computer Law & Security Review* 44 (2022): 105638.

¹³⁵ *Ibid.*

¹³⁶ *Ibid.*

¹³⁷ Banisar, D & Davies, S. "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments." *J. Marshall J. Computer & Info. L.* 18 (1999): 1.

¹³⁸ *Ibid.*

¹³⁹ Gutwirth, *supra* note 89.

in its constitution.¹⁴⁰ Similarly, Bakibinga's¹⁴¹ research during the same period largely aligned with Bygrave's findings. A turning point came in 2010 when Mambi¹⁴² recognized South Africa, Mauritius, and Seychelles for having enacted comprehensive data privacy legislation, indicating a gradual yet evident shift towards acknowledging and addressing privacy and data protection. This evolving landscape gained further clarity with Greenleaf's¹⁴³ 2011 enumeration, which included additional countries like Angola, Benin, Burkina Faso, and others, showcasing a broader adoption of data privacy laws.¹⁴⁴ Greenleaf's subsequent updates revealed a more encouraging picture: by 2022, 35 of the 55 African countries had introduced privacy and data protection laws, marking a significant upturn in legislative activity.¹⁴⁵ By late 2021, about 60% of African countries had established data privacy laws, reflecting a continent-wide trend over the past two decades toward enacting and refining such legislation.¹⁴⁶ However, while this legislative expansion signals growing awareness, it does not necessarily equate to regulatory success. The proliferation of laws, particularly those modeled closely on external frameworks like the GDPR, raises important questions about contextual fit and actual implementation. Many of these laws lack local responsiveness, overlook cultural nuances, or remain unenforced due to institutional constraints. In this light, more legislation is not inherently beneficial unless it is both effective and contextually relevant. This emphasizes the need for a more critical assessment of not just how many laws exist, but how well they function in practice. Beyond national

¹⁴⁰ Bygrave, *supra* note 78.

¹⁴¹ Bakibinga, EM. "Regulating Market Entry in the Telecommunications Sector in an Integrated East Africa: Towards a Common Licensing Framework." Master's thesis.

¹⁴² Mambi, AJ. *ICT Law Book: A Source Book for Information and Communication Technologies & Cyber Law in Tanzania & East African Community*. African Books Collective, 2010.

¹⁴³ Greenleaf and Cottier, *supra* note 134.

¹⁴⁴ *Ibid.*

¹⁴⁵ *Ibid.*

¹⁴⁶ *Ibid.*

legislation, Africa has also seen the development of the African Union Convention on Cybersecurity and Data Protection and four regional multi-state data privacy instruments.¹⁴⁷

The literature indicates two primary forces driving the evolution of data privacy laws in Africa: international influences, such as the United Nations (UN) and the European Union (EU), and internal African developments.¹⁴⁸ The international dimension, especially the alignment with UN conventions and EU directives like the GDPR, highlights a global influence on African legal frameworks.¹⁴⁹ These external standards have served both as a model and a catalyst for African countries, guiding the creation and refinement of data privacy instruments that aspire to global benchmarks. African countries' engagement with the Council of Europe's Data Protection Convention 108,¹⁵⁰ being among the first to apply and be accepted for accession, highlights active participation in international data protection discourse. The diverse approaches to privacy protection, encompassing sub-regional initiatives, constitutional provisions, and sector-specific laws, reflect the multifaceted strategies African nations employ to navigate the complexities of data privacy and protection. The literature presents a diverse picture of data privacy regulation across Africa, highlighting a spectrum of approaches from comprehensive legislative frameworks in some countries to the absence of such laws in others. This variation highlights the emphasis on sub-regional initiatives, constitutional mandates, and sector-specific regulations, reflecting the continent's diverse strategy toward ensuring privacy protection.

2.3 Theoretical Framework

This thesis employs TWAIL as a critical framework to explore the intricacies of privacy and data protection within the African context. While TWAIL does not directly tackle the

¹⁴⁷ ECOWAS (west); SADC (south), ECCAS and CEMAC (central) and EAC (east).

¹⁴⁸ Banisar and Davies, *supra* note 136; Bakibinga, *supra* note 140; Mambi, *supra* note 141; Greenleaf and Cottier, *supra* note 134; Makulilo, *supra* note 71; Bygrave, *supra* note 104.

¹⁴⁹ *Ibid.*

¹⁵⁰ Greenleaf and Cottier, *supra* note 134.

issues of privacy and data protection, its foundational principles offer profound insights into these areas from the perspective of the Global South. By challenging the conventional paradigms of international law, TWAIL emphasizes the significance of incorporating experiences and viewpoints from the Global South into legal discourse.¹⁵¹ This approach not only questions the prevailing Western-centric narratives but also strives for a more equitable international legal order by shedding light on historical injustices and championing the rights and voices of marginalized communities and developing nations.¹⁵² TWAIL's dedication to examining the historical context of international law and acknowledging the autonomy of the Global South is instrumental in addressing the existing power imbalances and injustices within the international legal system.¹⁵³ Moreover, it advocates for ethical commitments to justice and equality, seeking to transform the international legal system into one that is fair, inclusive, and reflective of the world's diverse voices. The transformative potential of TWAIL is evident in its ability to shape international legal norms, promote inclusivity, challenge entrenched power structures, advocate for social justice, and incorporate a variety of legal traditions and viewpoints.¹⁵⁴ This not only critiques the current state of affairs but also offers innovative solutions to global challenges, aiming for a future where legal frameworks genuinely cater for the diverse needs and aspirations of the international community. Central to the TWAIL framework, as Obiora Chinedu Okafor¹⁵⁵ articulates, is a collective ethical commitment among TWAIL scholars to confront and reform aspects of the international legal system that sustain global inequalities and injustices. This commitment highlights the

¹⁵¹ Mutua, Makau wa. "Savages, Victims, and Saviors: The Metaphor of Human Rights." *Harvard International Law Journal* 42 (2001): 201-234; Chimni, B.S. "Third World Approaches to International Law: A Manifesto." *Third World Quarterly* 27, no. 5 (2006): 767-776; Okafor, Obiora Chinedu. "Critical Third World Approaches to International Law (TWAIL): Theory, Methodology, or Both?" *International Community Law Review* 10 (2008): 371-378; Mutua, Makau & Anghie, Antony. "What Is TWAIL?" *Proceedings of the Annual Meeting (American Society of International Law)*, vol. 94, April 5-8, 2000, pp. 31-40. Cambridge University Press on behalf of the American Society of International Law.

¹⁵² *Ibid.*

¹⁵³ *Ibid.*

¹⁵⁴ *Ibid.*

¹⁵⁵ Okafor, Obiora Chinedu. "Newness, Imperialism, and International Legal Reform in Our Time: A TWAIL Perspective." *Osgoode Hall Law Journal* 43 (2005): 171.

necessity of valuing the experiences of the Global South and marginalized groups above traditional Western-centric methods. Okafor elucidates this point in his article “*Newness, Imperialism, and International Legal Reform in Our Time: A TWAIL Perspective*,” stating:

TWAIL scholars (or ‘TWAILers’) are solidly united by a shared ethical commitment to the intellectual and practical struggle to expose, reform, or even retrench those features of the intellectual legal system that help create or maintain the generally unequal, unfair, or unjust global order., a commitment to centre the rest rather than merely the west, thereby taking the lives and experiences of those who have self-identified as Third World much more seriously than has generally been the case.¹⁵⁶

At the core of TWAIL is a unified stance against the unjust global order, encapsulating both intellectual and political opposition. Makau Mutua¹⁵⁷ succinctly describes TWAIL’s objectives:

The first is to understand, deconstruct, and unpack the uses of international law as a medium for the creation and perpetuation of a racialized hierarchy of international norms and institutions that subordinate non-Europeans to Europeans. Second, it seeks to construct and present an alternative normative legal edifice for international governance. Finally, TWAIL seeks through scholarship, policy, and politics to eradicate the conditions of underdevelopment in the Third World.¹⁵⁸

TWAIL’s critical legal theory also explores the intersectionality of oppression spanning race, gender, class, and colonial legacies within international law, acknowledging that legal norms are deeply intertwined with broader social, economic, and cultural structures.¹⁵⁹ It scrutinizes how these varied forms of marginalization intersect, significantly influencing the Global South’s communities and individuals. Moreover, TWAIL critiques the Eurocentric and colonial bases of the current legal order, spotlighting the power dynamics and structural inequalities that favour Western states while often sidelining the Global South.¹⁶⁰ It champions a contextual analysis of international law, arguing against the universal application of legal principles without consideration for the Third World countries’ unique contexts.¹⁶¹ This perspective promotes a more inclusive understanding of international law,

¹⁵⁶ *Ibid.*, 176-177.

¹⁵⁷ Mutua, Makau & Anghie, Antony. "What Is TWAIL?" *Proceedings of the Annual Meeting (American Society of International Law)*, vol. 94, April 5-8, 2000, pp. 31-40.

¹⁵⁸ *Ibid.*, 31.

¹⁵⁹ Chimni, B.S. "Third World Approaches to International Law: A Manifesto." *Third World Quarterly* 27, no. 5 (2006): 767-776.

¹⁶⁰ *Ibid.*

¹⁶¹ *Ibid.*

challenging Eurocentric and Western-centric views. By integrating TWAIL principles, this thesis aims to uncover a nuanced and comprehensive understanding of how privacy and data protection can be regulated within Africa, acknowledging the importance of selecting TWAIL theories that resonate most closely with the thesis objectives. This selective engagement ensures the thesis remains focused on aspects that directly inform the analysis of privacy and data protection in the African context, striving for a legal framework that is equitable, just, and truly reflective of the diverse African narratives.

2.3.1 Navigating Through TWAIL and the Legacy of Colonialism

This thesis is grounded in TWAIL, focusing keenly on dissecting the enduring colonial legacies that have significantly shaped the legal frameworks and power constructs across the Global South. This inquiry transcends academic curiosity, targeting a profound understanding of how these historical imprints persistently mould the current legal frameworks, with a particular lens on privacy and data protection regulations within Africa. Central to TWAIL is the recognition of colonialism's lasting impacts, evident not just in enduring forms of domination but also through the emergence of contemporary governance structures that mirror those of the colonial and pre-colonial eras.¹⁶² This intricate web of historical influences is pivotal for analyzing the evolution of privacy and data protection legislation in Africa, shedding light on the significant challenges posed by predominantly Eurocentric legal frameworks to the sovereignty of African legal systems. Chapter 3 explores deeply into these issues, scrutinizing the cultural subjugation that emerges from the imposition of European standards, like the GDPR, on African countries. This imposition frequently eclipses regional efforts toward crafting data protection frameworks that genuinely resonate with African values and principles. Moreover, the lack of an Afrocentric perspective in existing regional

¹⁶² Koskeniemi, Martti. "Histories of International Law: Dealing with Eurocentrism." *Rechtsgeschichte - Legal History* 19 (2011): 152-176.

data protection initiatives¹⁶³ starkly highlights a broader narrative of cultural erasure and the sidelining of indigenous legal philosophies in the formation of standards.

By applying TWAIL's analytical lens, this thesis critically examines the colonial foundations that continue to underpin global governance systems, unveiling the power disparities and historical injustices that inform current legal practices and regulatory strategies. Luis Eslava and Sundhya Pahuja consider colonialism to extend beyond its historical occurrences; they view it as an enduring, influential factor that still dictates power structures, shapes legal norms, and affects interpersonal relationships within the sphere of international law.¹⁶⁴ Through their postcolonial perspective, Eslava and Pahuja bring to the fore the persistent influence of colonial residues on current international legal practices and the daily lives of individuals globally. They assert:

The 'post' of a 'postcolonial' international law is therefore a marker of continues yet spectral, presence of 'colonialism', and of the way its 'history' is still with us in discursive, ideological, and material terms. An attention to postcolonialism accordingly invites a constant re-examination of the different ways in which the world is still haunted by the modes of understanding, relating, and extracting that emerged in explicitly 'colonial' times.¹⁶⁵

Embracing this postcolonial framework is pivotal for examining the persistent echoes of colonialism's impact. Eslava and Pahuja draw attention to the importance of an ongoing critique of colonial rule and its enduring influence on international legal norms and institutions. They further elaborate:

...because colonialism is a process that has always been accompanied by multiple forms of resistance, (post)colonialism also forces an attention to how popular revolts, formal claims of self-government, and everyday acts of rebellion are also at the bosom of centre-periphery relations. For international lawyers specifically, an attention to (post)colonialism as a phenomenon invites us to think about the role of (international) law in the maintenance, as well as in the contestation, of colonial patterns of relations.¹⁶⁶

Incorporating this theoretical stance, this thesis explores the predominance of Western-centric legal doctrines, advocating for a reconceptualization of privacy and data protection

¹⁶³ Makulilo, *supra* note 71.

¹⁶⁴ Eslava, Luis, and Sundhya Pahuja. "Beyond the (Post)Colonial: TWAIL and the Everyday Life of International Law." *Verfassung und Recht in Übersee / Law and Politics in Africa, Asia and Latin America* 45, no. 2 (2012): 195-221. Nomos Verlagsgesellschaft mbH.

¹⁶⁵ *Ibid.*, 198.

¹⁶⁶ *Ibid.*

laws that resonate with African historical, cultural, and societal intricacies. By anchoring the analysis in the TWAIL framework, this thesis forges a nexus between international legal standards and the experiences of African countries. It promotes regulatory systems that are not only fair but also acutely cognizant of Africa's multifaceted realities. Consequently, this inquiry substantially enriches the dialogue on privacy and data protection, guiding the creation of legal frameworks that are equitable, suited to the digital age's challenges, and deeply ingrained in the unique African cultural and historical narrative. Such an approach does more than advance academic discourse; it paves the way for the establishment of legal protocols that mirror and respond to the distinctiveness of the African context. Within this context, TWAIL's critique of Eurocentrism becomes particularly salient.

2.3.2 TWAIL's Critique of Eurocentrism

Within the scope of this thesis, the critique of Eurocentrism, as posited by TWAIL, provides an essential foundation for scrutinizing the GDPR and its application in the African context. Through a critical examination, TWAIL scholars interrogate the prevalent Eurocentric biases in international law, which predominantly favour Western perspectives and norms at the cost of the sovereignty, rights, and well-being of the Global South.¹⁶⁷ This critical perspective is vital, recognizing that the gestation and execution of international law have largely served Western interests, often sidelining the perspectives and needs of non-Western states and communities. Eurocentrism, lacking a precise and explicit definition in the scholarly domain, is adeptly critiqued by Martti Koskenniemi¹⁶⁸ among others, who unravel its manifestations within international law and its consequential effects on historical narratives and viewpoints. In this thesis, Eurocentrism is conceptualized as the inclination towards positioning Europe, or broadly, Western civilization, at the epicentre of historical,

¹⁶⁷ Mutua, *supra* note 150; Chimni, *supra* note 150; Okafor, *supra* note 150; Mutua and Anghie, *supra* note 150.

¹⁶⁸ Koskenniemi, *supra* note 161.

cultural, and intellectual discourses, frequently sidelining or marginalizing non-Western perspectives and contributions.¹⁶⁹ Specifically, in the realm of privacy and data protection, Eurocentrism signifies the preeminence of European perspectives, values, norms, and legal frameworks in dictating global standards and practices, notably through instruments like the GDPR. This Eurocentric dominance often disregards the cultural, social, legal, and economic contexts of other regions, particularly the Global South, potentially leading to challenges in non-European contexts, especially within Africa.¹⁷⁰ This Eurocentric approach manifests notably in regulatory frameworks and the conceptualization of privacy, where European regulations such as the GDPR are heralded as global benchmarks. While these laws establish high standards, their application as universal models without due consideration of the diverse socio-cultural and legal contexts across Africa raises significant issues regarding enforceability, relevance, and potential conflicts with local customs and norms surrounding privacy. This dichotomy extends to the individual-centric view of privacy prevalent in European and Western contexts, which may not harmonize with the communal or collective perspectives on privacy prevalent in many non-Western societies, where community interests and social harmony may supersede individual privacy rights.¹⁷¹

TWAIL scholars critically emphasize how Eurocentrism in international law not only cements unequal power dynamics but also perpetuates neo-colonial structures, effectively marginalizing the unique legal traditions, values, and needs of societies outside the Western world.¹⁷² They call for a shift in legal scholarship towards a more inclusive and expansive approach, a sentiment powerfully echoed by Ian Hunter when he remarks:

¹⁶⁹ *Ibid.*

¹⁷⁰ Tzouvala, Ntina. "The Specter of Eurocentrism in International Legal History." *Yale Journal of Law & the Humanities* 31, no. 2 (2021): 413-433.

¹⁷¹ Bygrave, *supra* note 81.

¹⁷² Mutua, *supra* note 150; Chimni, *supra* note 150; Okafor, *supra* note 150; Mutua and Anghie, *supra* note 150; Fidler, David P. "Revolt Against or From Within the West?: TWAIL, the Developing World, and the Future Direction of International Law." *Articles by Maurer Faculty*, 2003. Available at: <https://www.repository.law.indiana.edu/facpub/2126>.

... far from being global, the law of nature and nations represented a Eurocentric normative order, as it had emerged to resolve a historically specific intra-European cultural and political problem: how to regulate war- and peacemaking once the fracturing of Christianity – including its Thomistic metaphysics – and the emergence of territorial states had put an end to any lingering *respublica Christiana*.¹⁷³

Hunter's insights underline the critical need for legal scholarship to broaden its perspective, integrating the diverse and rich viewpoints from the Global South to ensure a more comprehensive and representative understanding of international law. Further illuminating the critique of Eurocentrism, Anghie¹⁷⁴, as referenced in Makau wa Matua's insightful article "*Savages, Victims, and Saviors: The Metaphor of Human Rights*", articulates the consequences of imposing a Eurocentric worldview on the discipline of international law:

..The extension and universalization of the European experience, which is achieved by transmuting it into the major theoretical problem of the discipline [international law], has the effect of suppressing and subordinating other histories of international law and the people to whom it has applied. Within the axiomatic framework of positivism, which decrees that European states are sovereign while non-European states are not, there is only one means of relating the history of the non-European world, and this the positivists proceed to do: it is a history of the civilizing mission, the process by which peoples of Africa, Asia, the Americas, and the Pacific were finally assimilated into a European international law.¹⁷⁵

The above mentioned profound critiques spotlight the essential task confronting legal scholars: to transcend the limitations of a Eurocentric approach and embrace a narrative that acknowledges and values the multiplicity of experiences and legal philosophies that exist worldwide. By doing so, international law can evolve into a truly global discipline that reflects the realities and respects the sovereignty of all societies, not just those within the Eurocentric sphere. The relevance of this critique becomes even more pronounced when considering the GDPR, a regulation conceived and developed through a purely European lens, without input from African countries. The exclusion of African perspectives during the GDPR's formulation prompts critical questions regarding its relevance and adaptability to the African context, characterized by its distinct cultural, social, and economic realities.

¹⁷³ Hunter. "Global Justice and Regional Metaphysics. On the Critical History of the Law of Nature and Nations." *In Law and Politics in British Colonial Thought: Transpositions of Empire*, edited by S. Dorsett and I. Hunter, 13-20. Basingstoke: Palgrave Macmillan, 2010.

¹⁷⁴ Mutua, *supra* note 150.

¹⁷⁵ *Ibid.*, 234-235.

Through the TWAIL perspective, this thesis explores the barriers and challenges associated with applying the GDPR in Africa, underlining the imperative for a regulatory framework that genuinely mirrors and respects the continent's unique identity and values. Emphasizing cultural diversity and advocating for the inclusion of marginalized voices from the Global South, this thesis highlights existing African approaches to privacy and data protection that align with communal values and collective welfare. It advocates moving beyond the mere transplantation of Western legal frameworks to strengthening local practices that conform to international standards yet remain faithful to African cultural and societal norms. The transformative mission of TWAIL endorses the tailoring of privacy and data protection laws to accommodate the specific cultural, social, and economic nuances of Africa. This strategy aims to cultivate a richer understanding of how African views on community and individual identity might shape more suitable approaches to consent, data ownership, and the equilibrium between individual liberties and communal responsibilities. By weaving TWAIL's critical insights throughout this thesis, the objective is to make a meaningful contribution to the global discourse on privacy and data protection, forging a legal framework that not only meets international criteria but is also deeply rooted in the cultural spirit of Africa, guaranteeing its applicability, sustainability, and cultural authenticity.

2.3.3 Dependency Theory

Within the academic discourse on economic and sociological development, Dependency Theory offers a seminal perspective on the disparate growth trajectories between developed and developing nations.¹⁷⁶ It posits that the economic advancement of developing countries is significantly influenced and often hampered by their dependence on more developed nations. This dependency manifests itself across various dimensions, including the need for resources,

¹⁷⁶ Anghie, *supra* note 150; Chimni, *supra* note 150; Mutua and Anghie, *supra* note 150; Koskenniemi, *supra* note 161.

technology, and access to markets, which collectively contribute to a cycle of underdevelopment and economic exploitation.¹⁷⁷ At the core of Dependency Theory is the critique of structural inequalities within the global economic system.¹⁷⁸ These inequalities are seen as being intentionally configured to advantage developed nations at the detriment of developing ones.¹⁷⁹ The theory argues that the international division of labour and trade relations are skewed to favour the interests of dominant powers, consequently relegating less powerful states to a position of marginalization and dependency.¹⁸⁰ This critique gains further depth through the analysis provided by Makau Mutua and Antony Anghie,¹⁸¹ who draw on Nyerere's insights to highlight the exploitative nature of the international legal and economic order. Nyerere poignantly articulates the plight of the Third World, which, despite its significant population and control over crucial raw materials, finds itself marginalized in global economic governance. He says:

The Third World consists of the victims and the powerless in the international economy Together we constitute a majority of the world's population and possess the largest part of certain important raw materials, but we have no control and hardly any influence over the manner in which the nations of the world arrange their economic affairs. In international rule-making, we are recipients, not participants.¹⁸²

Furthermore, the theory analyses the enduring effects of colonialism and imperialism, identifying these historical epochs as foundational to the persistent economic dynamics and dependencies between former colonies and colonizers.¹⁸³ Responding to these challenges, Dependency Theory advocates for a fundamental overhaul of the global economic architecture. It champions policies that encourage economic sovereignty and self-reliance

¹⁷⁷ Mutua and Anghie, *supra* note 150.

¹⁷⁸ *Ibid.*

¹⁷⁹ *Ibid.*

¹⁸⁰ *Ibid.*

¹⁸¹ *Ibid.*

¹⁸² *Ibid.*, 35; Nyerere, Julius K. "South-South Option." *In The Third World Strategy: Economic and Political Cohesion in the South*, edited by Altaf Gauhar, 9-10. 1983.

¹⁸³ Mutua and Anghie, *supra* note 150.

among developing nations, aiming for a recalibration of trade relations to dismantle the power imbalances and dependencies that have historically disadvantaged the Global South.¹⁸⁴

Within the framework of this thesis, Dependency Theory as interpreted through the lens of TWAIL offers a profound critique of the global legal and economic order, particularly illuminating the dynamics of dependency between the Global North and the Global South. Originating in the 1960s, Dependency Theory emerged as a critical response to the glaring economic and political disparities between developed and developing nations, positing that the international system is structured in a way that perpetuates the economic reliance of less developed countries on their more developed counterparts.¹⁸⁵ This theory points out the historical role of the Global South as a reservoir of raw materials and cheap labour, with the Global North dominating in areas such as decision-making, technological advancement, and capital accumulation.¹⁸⁶ The critique extends to the legal instruments that maintain this economic imbalance, including international trade agreements, investment treaties, and intellectual property regimes, which often favour the interests of multinational corporations and affluent states at the expense of the Global South.¹⁸⁷

Furthermore, Dependency Theory within the TWAIL framework also casts a critical eye on the roles of international institutions such as the World Bank, the International Monetary Fund (IMF), and the World Trade Organization (WTO) in sustaining economic dependencies.¹⁸⁸ Advocating for a radical rethinking of the international economic and legal orders, TWAIL scholars call for reforms that directly confront and aim to rectify the entrenched inequalities and dependencies faced by the Global South. They champion a legal and economic system that genuinely recognizes and facilitates the sovereignty, self-

¹⁸⁴ *Ibid.*

¹⁸⁵ *Ibid.*

¹⁸⁶ *Ibid.*

¹⁸⁷ *Ibid.*

¹⁸⁸ *Ibid.*, 35.

determination, and developmental goals of the Global South.¹⁸⁹ Furthermore, echoing the broader tenets of TWAIL, Dependency Theory emphasizes the critical necessity of amplifying the voices and perspectives of the Global South within international legal conversations. It advocates for the meaningful involvement of developing nations in the formulation of policies, decision-making processes, and the crafting of international legal standards. Incorporating the TWAIL Dependency Theory into the research framework of this thesis offers a critical lens through which to examine the specific challenges and implications of implementing the GDPR within the African context. By applying the insights gleaned from Dependency Theory, this thesis dissects the structural economic and legal disparities that may influence the efficacy and appropriateness of the GDPR for African countries, thereby addressing the overarching research question: *What are the implications and challenges of adopting and implementing the GDPR in the African context, and how can TWAIL perspectives inform the development of a contextually appropriate regulatory framework?*

Dependency Theory, as interpreted through TWAIL, provides a valuable lens for analyzing how global legal and economic structures impact Africa's capacity to adopt and implement the GDPR. It highlights how systemic economic dependencies, reinforced through legal instruments and global institutions, limit African countries' autonomy in crafting data protection regimes that align with their socio-economic realities.¹⁹⁰ Rather than easing inequalities, the GDPR's stringent enforcement requirements risk deepening them. For example, compliance demands,¹⁹¹ such as advanced infrastructure and expert personnel, place disproportionate pressure on governments still building digital economies. This may lead to a diversion of resources away from critical development priorities like health and education.

¹⁸⁹ Anghie, *supra* note 150; Chimni, *supra* note 150; Mutua and Anghie, *supra* note 150; Koskenniemi, *supra* note 161.

¹⁹⁰ *Ibid.*

¹⁹¹ 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 (General Data Protection Regulation), [2016] OJ, L 119/1, arts 5, 24-43, 77-84.

Furthermore, by imposing hefty fines for non-compliance, the GDPR risks stifling innovation and discouraging the growth of African digital startups, which may lack the financial capacity to adhere to these requirements, thereby limiting local economic opportunities. This analysis also extends to the operational context of data privacy within Africa. Many states remain reliant on external data processors, further entrenching dependency and limiting data sovereignty.¹⁹² This weakens opportunities for cultivating local tech ecosystems and reinforces economic asymmetries. A dependency-informed critique thus reframes privacy regulation not only as a rights-based legal issue but as a core component of economic self-determination. By integrating Dependency Theory within TWAIL's broader critique, this thesis proposes a privacy and data protection model for Africa that moves beyond compliance to address systemic imbalances.

2.3.4 Human Rights and Social Justice

In the realm of Human Rights and Social Justice, the TWAIL framework provides an essential perspective for analyzing privacy and data protection, particularly as they pertain to the African context. TWAIL's examination of human rights discourse sheds light on the embedded limitations, biases, and power dynamics that often skew mainstream human rights frameworks.¹⁹³ This critique is instrumental in advocating for a more inclusive, context-sensitive, and transformative approach to understanding and applying human rights, including those related to privacy and data protection. Privacy and data protection are intrinsically linked to human rights, particularly the right to dignity, freedom of expression, and the right to information.¹⁹⁴ In Africa, where societies often prioritize communal values and collective identities, privacy protections must be understood within the broader

¹⁹² Bryant, *Africa in the Information Age*. (2021). *Stanford Technology Law Review*, vol 24, p. 410-412.

¹⁹³ Mutua, *supra* note 150.

¹⁹⁴ Mendel, Toby. "The Right of the Public to Know and Freedom of Expression: Information Seen from the Consumer's Angle." Conference on Freedom of Expression and the Right to Privacy, 23 September 1999, Strasbourg, *Article 19*.

framework of social justice and the right to autonomy over personal and collective information. Privacy violations, especially in the digital age, can undermine individuals' rights to freedom of speech, association, and participation in public life.¹⁹⁵ This is particularly important in the African context, where data misuse, surveillance, and lack of comprehensive privacy frameworks disproportionately affect marginalized communities, thus exacerbating existing inequalities.¹⁹⁶ These considerations underline the unique human rights implications of privacy and data protection in Africa, where safeguarding privacy is not merely an individual right but a collective necessity tied to the socio-economic realities of African states.

TWAIL scholars reinforce the dominance of the Global North's perspectives in shaping traditional human rights discourses, frequently overlooking the unique experiences, priorities, and struggles of marginalized communities in the Global South.¹⁹⁷ This oversight extends to privacy and data protection, where Eurocentric notions of rights and individualism have often overshadowed collective identities and social justice considerations inherent to many African societies.¹⁹⁸ While the direct applicability of this theory to privacy and data protection is acknowledged as limited within this thesis, it provides valuable insights into contextualizing rights. TWAIL advocates for a nuanced understanding of human rights that considers the historical, social, cultural, and economic contexts of the Global South.¹⁹⁹ This approach emphasizes that rights, including those related to privacy and data protection, cannot be universally applied without adaptation to local contexts. It calls for the recognition of diverse rights, traditions and community-based approaches, reflecting the specific needs and aspirations of different societies. Furthermore, the TWAIL perspective on human rights acknowledges the intersecting forms of oppression and discrimination faced by marginalized

¹⁹⁵ Mutua, *supra* note 150.

¹⁹⁶ *Ibid.*

¹⁹⁷ Mutua, *supra* note 150; Chimni, *supra* note 150; Okafor, *supra* note 150; Mutua and Anghie, *supra* note 150.

¹⁹⁸ *Ibid.*

¹⁹⁹ Anghie, *supra* note 150.

groups in the Global South.²⁰⁰ It highlights the critical need to address systemic inequalities and structural violence that perpetuate marginalization, which is equally relevant in discussions about privacy and data protection.²⁰¹

Economic, social, and cultural rights are also emphasized by TWAIL scholars as essential to the comprehensive understanding of human rights. TWAIL scholars argue for the interconnectedness of civil, political, and socioeconomic rights, critiquing the mainstream human rights discourse's tendency to prioritize the former over the latter.²⁰² This critique is pertinent to privacy and data protection, as the effective realization of these rights often hinges on the fulfillment of broader socioeconomic rights. For instance, without access to adequate infrastructure, education, and resources, individuals and communities may not be able to fully exercise their rights to privacy and data protection. Limited access to digital technologies or lack of data literacy disproportionately affects marginalized groups in Africa, making them more vulnerable to data exploitation and privacy violations. As a result, addressing privacy rights in isolation from socioeconomic conditions risks perpetuating existing inequalities. Makau wa Mutua's insights further enrich this discourse. He stresses the importance of embracing cultural diversity in critiquing human rights and calls out the inadequacies of the current human rights framework. He states:

...The critique of human rights should be based not just on American or European legal traditions but also on other cultural milieus. The indigenous, non-European traditions of Asia, Africa, the Pacific, and the Americas must be central to this critique. The idea of the human rights quest to craft a universal bundle of attributes with which all societies must endow all human beings is a noble one. The problem with the current bundle of attributes lies in their inadequacy, incompleteness, and wrong-headedness. There is little doubt that there is much to celebrate in the present human rights corpus just as there is much to quarrel with. In this exercise, a sober evaluation of the current human rights corpus and its language is not an option-it is required.²⁰³

In synthesizing these insights with the research focus on privacy and data protection, this thesis draws on TWAIL's critique of Human Rights and Social Justice to argue for a privacy

²⁰⁰ *Ibid.*

²⁰¹ *Ibid.*

²⁰² Anghie, *supra* note 150; Chimni, *supra* note 150; Mutua and Anghie, *supra* note 150; Koskenniemi, *supra* note 161.

²⁰³ Mutua, *supra* note 150

and data protection framework that is contextually relevant to Africa. Such an approach has the potential to fill the void in the Eurocentric human rights corpus posed by African cultural realities, at least in the context of the quest to design an African-sensitive privacy and data protection architecture and its intersection with a culturally inclusive human rights framework. It seeks to transcend Eurocentric models by incorporating Indigenous and non-European legal traditions, advocating for a more equitable and culturally sensitive approach that aligns with the continent's diverse social, cultural, and economic realities. Through this lens, the thesis aims to contribute to developing privacy and data protection norms that not only respect global standards but also embody the principles of social justice and the realities of the Global South.

2.4 Conclusion

In concluding this chapter, a detailed narrative is presented, combining cultural, legal, and technological elements that shape the current state of privacy and data protection in Africa. The analysis acknowledges the essential role of privacy, not just as a personal right but as a crucial aspect of societal well-being, deeply connected with the continent's diverse cultural and religious backgrounds. It points out the significant legal progress made towards enhancing privacy protections but also highlights ongoing challenges in enforcement. These challenges point to a gap between the development of policies and their actual implementation. Through the lens of TWAIL, the chapter explores the lasting effects of colonial legacies and power imbalances on African legal frameworks and privacy norms. By questioning Eurocentrism and supporting indigenous viewpoints, TWAIL provides valuable insights for developing legal frameworks that better match Africa's unique social, cultural, and legal environments. This approach encourages a move away from dominant narratives

towards a more inclusive and fair legal order, emphasizing the need to integrate rights within the African historical, social, and cultural contexts.

The discussion on culture, privacy, and data protection sheds light on the complex relationship between communal values and the understanding of privacy in African societies. It suggests moving beyond simple comparisons of Western individualism and African communalism towards a more nuanced view of privacy that respects the continent's diverse cultures. The impact of Information and Communication Technologies and the evolution of data protection laws are also examined, highlighting the proactive efforts towards stronger privacy protections in response to digital advancements. Additionally, considering the role of religious beliefs and development priorities offers a wider perspective on the challenges and opportunities for aligning global privacy standards with local realities. This chapter sets a solid foundation for further investigation into privacy and data protection in Africa, suggesting a path toward legal and regulatory frameworks that are fair, equitable, and reflective of the continent's rich cultural diversity. The insights gained from this analysis aim to ensure that future research is grounded in the African context, informed by a critical theoretical perspective, and contributes to a legal landscape that is inclusive and respects global diversity. This foundation leads into the next chapter, which examines the challenges and limitations of implementing the GDPR to create comprehensive privacy and data protection laws in Africa. It looks at the legal, cultural, technological, and institutional barriers African countries face in adopting and implementing the GDPR, and discusses how these impact the effectiveness of privacy and data protection regulations.

Chapter 3: Complexities of Transplanting GDPR into African Legal Frameworks

3.1 Introduction

The advent of the digital age has significantly transformed the realm of privacy and data protection, leading to the EU's enactment of the GDPR on May 25, 2018. This landmark regulation, which was officially adopted on May 24, 2016, and became effective on May 25, 2018, exercises binding legal force throughout the EU member states.²⁰⁴ The GDPR represents a significant evolution in European privacy and data protection legislation, replacing the previous Data Protection Directive 95/46/EC.²⁰⁵ Its primary aim is to streamline data protection laws across Europe, thereby enhancing privacy rights for individuals in an era characterized by swift technological advancements.²⁰⁶ At the heart of the GDPR are fundamental principles such as accountability,²⁰⁷ transparency,²⁰⁸ and the adoption of stringent data protection measures.²⁰⁹ These principles underpin the regulation's commitment to safeguarding personal data and empowering individuals with several enforceable rights. These rights include but are not limited to, the ability to challenge data processing,²¹⁰ request the deletion of personal data (also known as the right to be forgotten),²¹¹ to correct inaccurate information,²¹² and to gain insights into data processing practices.

²⁰⁴ Regulation 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 Council Directive 95/46/EC, 2016 O.J. (L 119) 1 (EU) (hereinafter GDPR).

²⁰⁵ *Ibid.*

²⁰⁶ *Ibid.*

²⁰⁷ GDPR, Article 24(1).

²⁰⁸ GDPR, Article 12.

²⁰⁹ GDPR, Article 32.

²¹⁰ GDPR, Article 21.

²¹¹ GDPR, Article 17.

²¹² GDPR, Article 16.

To ensure compliance with the above-mentioned rights, the GDPR places rigorous requirements on organizations involved in digital interactions with EU citizens. Data collection practices are restricted to what is strictly necessary for clearly defined purposes,²¹³ and data handlers are compelled to implement protective measures like encryption and obtain cyber liability insurance.²¹⁴ Additionally, the regulation mandates that organizations must inform regulatory authorities about data breaches within 72 hours of their occurrence.²¹⁵ Compliance with the GDPR is not only a legal obligation for entities dealing with EU residents but also a prerequisite for maintaining access to one of the world's largest economic blocs, as non-compliance can result in severe penalties, including restricted market access.²¹⁶

Consequently, the GDPR serves to protect individual rights and standardize data protection laws across the EU, promoting a cohesive approach to privacy regulation in the digital sphere. It imposes significant penalties for violations, highlighting the EU's dedication to comprehensive personal data protection.²¹⁷ This legislative initiative reflects the EU's proactive response to evolving demands in data protection. The ramifications of the GDPR extend well beyond the borders of Europe, compelling countries globally, including those in Africa, to overhaul their privacy and data protection laws to align with its demanding standards.²¹⁸ The GDPR embodies the EU's ambition to set a worldwide standard for data protection that goes beyond the confines of its member states. In 2017, Vera Jourová, the European Commissioner for Justice, articulated the EU's intention to position the GDPR as a global benchmark.²¹⁹ This ambition is realized through two principal mechanisms: the regulation applies to any non-EU entity that monitors the behaviour of individuals in the

²¹³ GDPR, Article 5.

²¹⁴ GDPR, Article 32.

²¹⁵ GDPR, Article 33 (1).

²¹⁶ Scott, Mark, and Laurens Cerulus. "Europe's new data protection rules export privacy standards worldwide." *Politico*, January 31, 2018, 12:00 PM CET. Accessed April 17, 2024. <https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/>.

²¹⁷ GDPR, Article 83 (5).

²¹⁸ Scott and Cerulus, *supra* note 216.

²¹⁹ *Ibid.*

EU,²²⁰ such as through online tracking, and it affects any organization providing goods or services to EU residents, irrespective of the location of financial transactions.²²¹ Achieving compliance with the GDPR can occur through the enactment of national legislation that mirrors its principles or through organizational measures designed to meet its criteria. For countries, the path to compliance involves developing legal frameworks that offer data protection at par with the GDPR, with assessments considering the substance of legislation, enforcement mechanisms, adherence to the rule of law, and commitments to international privacy and data protection standards.²²² On the other hand, corporations can reach compliance through the formulation of internal policies and procedures or by engaging subcontractors that adhere to GDPR-compliant data security measures.²²³

In particular, the EU's rigorous enforcement of GDPR compliance represents a powerful mechanism, placing considerable pressure on data controllers to meet its exacting standards or face exclusion from the valuable EU market.²²⁴ This dynamic positions the EU as a pivotal influencer in the realm of global privacy and data protection regulation, manifesting a form of *data imperialism*²²⁵ that overlooks the varied cultural, political, and economic realities outside its jurisdiction. This influence, identified as the Brussels Effect by Columbia Law Professor Anu Bradford, demonstrates the EU's economic clout in compelling countries worldwide to mirror its regulatory framework, irrespective of its compatibility with local contexts.²²⁶ Such a trend of *Europeanization* transcends the EU's geographical boundaries, urging global alignment with GDPR mandates.²²⁷ Nonetheless, this push for standardization neglects the distinctive needs and ambitions of regions such as Africa, where

²²⁰ *Ibid.*

²²¹ *Ibid.*

²²² *Ibid.*

²²³ *Ibid.*

²²⁴ Sebastian, Manu J. "The European Union's General Data Protection Regulation: How Will It Affect Non-Enterprises?" *Syracuse Journal of Science and Technology Law* 31 (2015): 216-218.

²²⁵ Scott & Cerulus, *supra* note 216.

²²⁶ Bradford, Anu. "The Brussels Effect." *Northwestern University Law Review* 107 (2015): 1.

²²⁷ Bradford, Anu. "Exporting Standards: The Externalization of the EU's Regulatory Power Via Markets." *International Review of Law and Economics* 42 (2015): 158, 170.

a more flexible regulatory framework may better support technological innovation and economic expansion.²²⁸

Moreover, the GDPR imposes challenges on Africa's trade and development through its stringent compliance requirements and wide-reaching implications. Organizations are tasked with comprehensive data management responsibilities, including the maintenance of records,²²⁹ prompt breach notification,²³⁰ and the appointment of Data Protection Officers,²³¹ presenting operational hurdles, especially for smaller businesses with constrained resources. The risk of incurring substantial fines of up to EUR 20 million or 4 percent of worldwide turnover²³² poses a significant financial threat, potentially stifling investment and innovation within Africa's burgeoning digital economy and trade sectors. Compounding these challenges are the GDPR's ambiguous stipulations, such as the indeterminate terms '*undue delay*' and a '*reasonable*' level of data protection, which inject further uncertainty into compliance efforts and may obstruct the development of coherent strategies for EU market engagement.²³³

Additionally, the expansive definition of personal identification information under the GDPR, coupled with its applicability to all EU citizens irrespective of the data processing entity's location, increases the regulatory load for African enterprises active in international commerce.²³⁴ This extensive obligation complicates participation in the global digital marketplace, potentially overshadowing local practices and impeding Africa's progress in formulating privacy and data protection norms that align with its unique trade and development aspirations. Viewed through the TWAIL lens, the enforcement of GDPR norms upon African states highlights the prevailing power imbalances within international law. It

²²⁸ *Ibid.*

²²⁹ GDPR, Article 30.

²³⁰ GDPR, Article 33.

²³¹ GDPR, Article 37(5).

²³² GDPR, Article 83(5).

²³³ Thomson Reuters. "Top Five Concerns for GDPR Compliance."

<https://legal.thomsonreuters.com/en/insights/articles/top-five-concerns-gdpr-compliance>.

²³⁴ *Ibid.*

accentuates a scenario where the prerogatives of dominant entities often override the interests and developmental goals of less influential regions. Therefore, while the GDPR establishes an esteemed global privacy and data protection standard, its unilateral application challenges Africa's sovereignty in formulating privacy and data protection legislation congruent with its unique socio-economic and cultural circumstances.

In the context of this chapter's examination of privacy and data protection, the demand by the EU for global alignment with its privacy and data protection standards presents a formidable obstacle for African countries aiming to preserve their access to the EU market. This requirement often compels African countries to adjust their values and economic policies to the rigorous conditions set by the GDPR, despite potential conflicts with their existing legal structures. Although the GDPR allows for some flexibility in its implementation, the EU's demand for equivalency necessitates a level of legal conformity that may surpass the indigenous frameworks of various countries. This issue is acutely observed in African countries, which face the daunting task of balancing their comparatively flexible regulatory approaches against the stringent demands of the GDPR. The EU's regulatory strategy, which effectively adopts a *take-it-or-leave-it* attitude, overlooks the distinct economic realities of different African countries, choosing instead to use its economic power to enforce a standardized concept of privacy and data protection worldwide.²³⁵ While aiming for uniformity in privacy and data protection practices, this method neglects the complex realities of African countries, where rigid regulations could impede rather than encourage technological and economic development.²³⁶ African countries, therefore, find themselves at a crossroads: to either adapt to the EU's standards, potentially compromising their developmental objectives or face the risk of being marginalized from the valuable EU market. However, this crossroads need not be a binary choice. A reconciliatory approach

²³⁵ Scott & Cerulus, *supra* note 216.

²³⁶ *Ibid.*

could involve African countries engaging selectively with GDPR principles, identifying and adapting elements that align with their own legal traditions, economic priorities, and cultural values. This form of strategic adaptation would allow for regulatory compatibility without full dependence, thereby preserving Africa's regulatory autonomy while remaining globally interoperable.

This context lays the groundwork for an in-depth analysis of the complex challenges and constraints faced by African countries in their efforts to align with the GDPR's requirements, examining the legal, cultural, technological, and institutional factors that influence the efficacy of privacy and data protection regulations across the continent. In line with this understanding, the chapter explores the hurdles of implementing the GDPR in Africa, centring on the first research question: What are the challenges and limitations of implementing the GDPR to establish comprehensive privacy and data protection laws in Africa? It investigates the diverse legal, cultural, technological, and institutional elements that shape data protection approaches throughout Africa. This investigation reveals the delicate equilibrium needed to integrate external regulations while adapting them to fit the varied African realities. Moreover, the chapter examines the significant challenge of applying Western-centric notions of privacy and data protection to the African context, highlighting the nuanced difficulties and obstacles that arise in striving to meet the GDPR's rigorous criteria within African environments. Through a detailed examination of the pressures and challenges related to GDPR compliance in Africa, this thesis illuminates the complex interplay involved in both adopting and adapting to the GDPR within African settings. In doing so, it also begins to identify contextually grounded strategies, such as regional collaboration, capacity building, and the development of hybrid legal frameworks, that could support the emergence of data protection systems more aligned with African realities while still engaging global norms.

This chapter is organized into four main sections, each dedicated to analyzing the challenges and limitations African countries face in aligning with the GDPR. It begins with an examination of the legal challenges inherent in reconciling domestic laws with the GDPR, considering the diverse legal systems across Africa. This part explores the complex interplay between national laws, rooted in customary practices and colonial influences, and the GDPR's stringent standards. It discusses the multifaceted nature of legal compliance, highlighting the difficulties of integrating privacy protections within a framework that often prioritizes communal over individual rights. The discussion then shifts to cultural considerations, scrutinizing how African societal norms impact the perception and implementation of privacy laws. This segment contrasts the collective ethos prevalent in African societies with the GDPR's emphasis on individual rights, highlighting the pivotal role of communal values such as harmony, interdependence, and collective responsibility. It articulates how these cultural principles inform unique approaches to privacy and data protection on the continent. Technological barriers constitute the third focus area, where the chapter addresses the significant infrastructural and developmental gaps that impede GDPR compliance efforts in Africa. It highlights the technological disparities between African countries and their European counterparts, emphasizing the particular strain on small and medium-sized enterprises (SMEs) pivotal to Africa's economic landscape. While addressing the technological barriers to GDPR compliance is crucial, it is not sufficient to resolve the broader challenges. The deeper misalignment between the GDPR's focus on individual rights and the communal values that are foundational to many African societies remains a significant obstacle. Therefore, any technological advancements must be accompanied by a comprehensive consideration of the cultural context in which these regulations are to be implemented.

The final section tackles the institutional challenges associated with enacting and enforcing GDPR-compatible legislation within Africa's diverse governance frameworks. Through a detailed analysis of regional variations and the practical limitations of transplanting the GDPR framework into national laws across Africa, the chapter emphasizes the persistent difficulties faced in striving for GDPR compliance within diverse regional contexts. It explores the financial and operational implications of GDPR compliance for African businesses, identifying the necessity for strategies that accommodate the continent's unique technological, economic, and cultural realities. Each section of the chapter emphasizes the multifaceted challenges and limitations African countries face in striving for GDPR compliance, from legal and cultural hurdles to technological and institutional barriers. These discussions reveal the critical need for adaptable strategies that not only align with global privacy and data protection standards but also resonate with the distinct contexts of African countries.

3.2 Overview of the GDPR

The development of the GDPR can be traced back to 1995 up to operationalization on May 25, 2018. Originating from the European Data Protection Directive (Directive 95/46/EC) that was established on October 24, 1995, the directive's initial purpose was to protect individual rights in the processing of personal data and to ensure the free flow of such data across borders.²³⁷ The journey toward the GDPR saw several key milestones, beginning with the European Data Protection Supervisor's opinion on the European Commission's Communication in June 2011, which highlighted the need for reform.²³⁸ This led to the European Commission's proposal in January 2012 to overhaul the EU's data protection

²³⁷ Regulation 2016/679, *supra* note 204.

²³⁸ European Data Protection Supervisor. "The History of the General Data Protection Regulation." Accessed from https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

framework. The legislative process gained momentum with the European Parliament's endorsement of the GDPR in March 2014, followed by the Council of the EU's agreement in June 2015.²³⁹ A pivotal moment was reached in December 2015 when the European Parliament, the Council, and the Commission arrived at a consensus on the GDPR's text. Officially adopted on April 27, 2016, as Regulation (EU) 2016/679, alongside Directive (EU) 2016/680 for data protection in the law enforcement sector, the GDPR was set to replace the previous directive and harmonize data protection across the EU. The GDPR came into force on May 24, 2016. This marked the point at which the regulation became legally binding, although it was not yet actively enforced. The GDPR was then applied from May 25, 2018, meaning that organizations were required to comply with its provisions from this date, marking the beginning of its full operationalization and enforcement. This period also saw proposals for enhancing privacy and electronic communications and updating data protection regulations for EU institutions in January 2017, further expanding the scope of data privacy.²⁴⁰

Additionally, the Data Protection Directive for the police and justice sectors was integrated into the national laws of EU member states by May 6, 2018, demonstrating the comprehensive reach of the EU's data protection efforts. The activation of the GDPR on May 25, 2018, represented a substantial evolution in the EU's approach to data protection.²⁴¹ It is important to note that the formation and enactment of the GDPR were driven exclusively by EU bodies, with no direct involvement from African nations, setting the stage for the discussions on the challenges African countries face in aligning with such regulations. Furthermore, the GDPR stands as a detailed regulatory framework, composed of 99 articles and further elucidated by 173 recitals. Jones & Kaminski point out that the GDPR is situated within a larger legal framework, integrating the EU Charter, additional EU and national

²³⁹ *Ibid.*

²⁴⁰ *Ibid.*

²⁴¹ *Ibid.*

privacy laws, guidance from EU privacy authorities, decisions from EU courts, and the foundational 1995 Data Protection Directive.²⁴² This regulation adopts an expansive view of personal data, covering not just identifiable information such as names and addresses but also pseudonymous and online identifiers.²⁴³ It also addresses the concept of data processing, which spans a variety of activities from collection and storage to use, analysis, and sharing.²⁴⁴ Importantly, the GDPR designates certain types of data such as health, genetic, sexual orientation, political opinions, and religious beliefs information, as specially protected due to their sensitive nature.²⁴⁵ Remarkably, the GDPR's applicability extends to all entities, including individuals, governments, and non-profit organizations, that process personal data.²⁴⁶

Moreover, the GDPR delineates six fundamental rights for EU residents in Articles 12 to 23. These rights enable individuals to access and amend their data held by organizations, delete their data (the right to be forgotten),²⁴⁷ transfer their data,²⁴⁸ dissent to its processing,²⁴⁹ and challenge decisions made through automated processing.²⁵⁰ Additionally, the GDPR delineates various obligations in Articles 24 to 43 for entities, including fulfilling these rights without delay,²⁵¹ conducting Data Protection Impact Assessments,²⁵² adhering to the principles of data protection by default and by design,²⁵³ employing encryption and pseudonymization,²⁵⁴ swiftly informing authorities and impacted individuals about data

²⁴² Jones, M. L., & Kaminski, M. E. "An American's Guide to the GDPR." *Denver Law Review* 98(1), 93 (2020).

²⁴³ GDPR, Article 4(1).

²⁴⁴ GDPR, Article 4(2).

²⁴⁵ GDPR, Article 9(1).

²⁴⁶ Jones and Kaminski, *supra* note 242.

²⁴⁷ GDPR, Article 17.

²⁴⁸ GDPR, Article 20.

²⁴⁹ GDPR, Article 21.

²⁵⁰ GDPR, Article 22.

²⁵¹ GDPR, Articles 33 & 34.

²⁵² GDPR, Article 35.

²⁵³ GDPR, Article 25.

²⁵⁴ GDPR, Article 32.

breaches,²⁵⁵ and appointing a data protection officer to supervise compliance efforts.²⁵⁶ While discussions on the GDPR often emphasize consent, it is but one of the six legal grounds for data processing outlined in Article 6(1). These grounds include consent, contractual necessities, legitimate interests, legal requirements, vital interests of the data subject, and public interest.²⁵⁷ It is acknowledged that the GDPR also authorizes processing on public-interest and legitimate interest grounds and provides research or statistical derogations with safeguards; this thesis emphasizes the individual rights strand because it is the aspect most directly transplanted and operationalized in African instruments. The principle of legitimate interest offers flexibility but requires that this interest does not outweigh the privacy rights of individuals, necessitating entities to perform a thorough assessment of their interests against individuals' privacy expectations.

Irrespective of the legal basis for data processing, entities must inform consumers about the processing purposes, the legal basis for processing, the data protection officer's contact details (if applicable), and the identities of any third parties receiving the data.²⁵⁸ Further, processing special category data and obtaining consent from minors are subject to additional safeguards as detailed in Articles 11 and 7, respectively. The GDPR mandates a stringent criterion for obtaining consent,²⁵⁹ necessitating a clear and affirmative action such as ticking a box on a website; implied consent through pre-ticked boxes or passive behaviour does not suffice.²⁶⁰ Individuals should find it as easy to withdraw consent as to give it, with organizations required to use clear and simple language when seeking consent, ensuring that it is specific to the processing purposes.²⁶¹ Additionally, consent must be voluntarily given,

²⁵⁵ GDPR, *Article 33* (2).

²⁵⁶ GDPR, *Article 37*.

²⁵⁷ GDPR, *Article 6*(1).

²⁵⁸ GDPR, *Article 13*.

²⁵⁹ GDPR, *Article 7*.

²⁶⁰ GDPR, *Recital 32*.

²⁶¹ GDPR, *Article 7* (3).

prohibiting the conditioning of services on consent where processing is not necessary.²⁶² Organizations are also compelled to keep records of consent to prove GDPR compliance.²⁶³

While this chapter is not intended to serve as a comprehensive exposition of the GDPR, it critically examines the Regulation's extraterritorial applicability. The GDPR's jurisdiction extends beyond the European Economic Area (EEA), comprising the EU Member States, Iceland, Liechtenstein, and Norway, highlighting its global influence on data protection practices. Article 45 of the GDPR sanctions the transfer of personal data to third countries that the European Commission has recognized as providing adequate protection, effectively incentivizing non-EU countries to align with GDPR standards. Up to the year 2024, the Commission has endorsed the data protection regimes of Andorra, Argentina, Canada (limited to commercial organizations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom, the United States (specific to commercial entities participating in the EU-US Data Privacy Framework), and Uruguay, for their compliance with GDPR and the Law Enforcement Directive (LED).²⁶⁴

Notably, except for the United Kingdom, the adequacy decisions for these jurisdictions do not encompass data transfers in the law enforcement sector, which are governed separately by Article 36 of Directive (EU) 2016/680.²⁶⁵ The Commission bears the ongoing responsibility to periodically reevaluate these adequacy decisions, a procedural obligation that originated under the former Directive 95/46/EC and persists under the current

²⁶² GDPR, *Article 7 (4)*.

²⁶³ GDPR, *Article 7 (1)*.

²⁶⁴ European Commission. "Adequacy Decisions." European Commission - European Data Protection, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. Accessed April 18, 2024.

²⁶⁵ European Parliament and Council of the European Union. "Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA." *Official Journal of the European Union* L 119 (2016): 89-131.

GDPR. These periodic reviews are instrumental to the Commission's regulatory function, and the findings are formally communicated to the European Parliament and the Council. In addition to Article 45, Articles 46 to 50 delineate supplementary data transfer mechanisms, such as adherence to standard contractual clauses approved by the European Commission, providing a comprehensive legal framework for international data exchange. While adequacy decisions demonstrate context-sensitive evaluation in practice, the present critique focuses on the operational experiences of African regulators navigating GDPR-aligned compliance systems, rather than asserting formal rigidity within the EU's adequacy framework.

Within this comprehensive legal framework for data exchange, the GDPR not only facilitates the flow of information but also strictly enforces compliance. The ramifications of GDPR non-compliance were starkly highlighted in May 2023 when Meta was levied a record fine of €1.2 billion for the unauthorized transfer of EU user data to the United States.²⁶⁶ This incident, alongside similar legal challenges faced by Google Analytics for data transfers across the Atlantic, emphasized the rigorous enforcement landscape of the GDPR.²⁶⁷ The governance of the GDPR is entrusted to the Data Protection Authorities (DPAs) within each EU member state, as stipulated in Articles 51 to 59. These authorities are tasked with the oversight of data processing activities and adjudication of complaints within their respective jurisdictions. Penalties under the GDPR are substantial, with companies at risk of incurring fines for serious breaches up to €20 million or 4% of their global annual turnover, whichever is greater.²⁶⁸

This stringent regulatory environment, characterized by significant fines as highlighted by specific high-profile cases, sets the stage for a deeper analysis of GDPR penalties. Reflecting on the Enforcementtracker.com data up to April 2024, the cumulative

²⁶⁶ European Data Protection Board. "1.2 billion euro fine for Facebook as a result of EDPB binding decision." Website. Accessed April 18, 2024. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en.

²⁶⁷ *Ibid.*

²⁶⁸ GDPR, Article 83 (5).

total of GDPR fines reached an astonishing €4.485 billion, with 2048 individual fines recorded.²⁶⁹ The GDPR's reach extends across various industries, requiring organizations to implement a comprehensive set of compliance measures. These measures include detailed record-keeping of all data processing activities,²⁷⁰ appointing a dedicated data protection officer,²⁷¹ establishing strong security protocols,²⁷² promptly reporting any data breaches,²⁷³ attentively managing consumer requests,²⁷⁴ and conforming strictly to established rules for data protection violations.²⁷⁵

3.2.1 Evaluating the Economic Impact of GDPR Non-Compliance on Diverse Entities

The financial implications of GDPR non-compliance are significant, as evidenced by high-profile cases and the aggregate fines recorded by regulatory bodies.²⁷⁶ These penalties highlight the strict enforcement approach of the European Union, with substantial economic repercussions for both multinational corporations and SMEs. The enforcement regime applies equally to all entities, demonstrating a broad-reaching approach to regulatory compliance.²⁷⁷ However, when viewed through a critical lens, this uniformity in enforcement raises important questions about the economic disparities it amplifies. In regions where SMEs dominate the economic landscape, such as Africa, the financial burden of compliance could be disproportionately heavy. The stringent requirements of GDPR often demand substantial investment in compliance mechanisms, which may strain the limited resources of smaller enterprises. The economic impact extends beyond direct fines. Indirect costs, such as the need

²⁶⁹ Enforcementtracker, "Statistics: Fines imposed over time," accessed April 20, 2024, <https://www.enforcementtracker.com/?insights>.

²⁷⁰ GDPR, Article 30.

²⁷¹ GDPR, Article 37.

²⁷² GDPR, Article 32.

²⁷³ GDPR, Article 33.

²⁷⁴ GDPR, Article 15.

²⁷⁵ GDPR, Article 6.

²⁷⁶ Enforcement Tracker. (2024). *GDPR fines insights: Cumulative fines and enforcement trends from July 2018 to April 2024*. Available at: <https://www.enforcementtracker.com/?insights>, Accessed 30 April 2024.

²⁷⁷ Ibid.

for legal expertise, compliance audits, and infrastructural upgrades, can significantly challenge smaller businesses in less economically robust regions.²⁷⁸ These pressures may reduce their competitive edge and inhibit growth, particularly in a global market increasingly governed by data protection norms shaped in the Global North. Despite some flexibility in GDPR provisions for SMEs, these measures are insufficient to offset the broader economic disparities inherent in its application.²⁷⁹ The regulatory framework thus risks entrenching economic vulnerabilities in regions with limited capacity to absorb the high costs of compliance. This dynamic invites reflection on the broader implications of adopting externally imposed regulatory frameworks in contexts where the economic realities differ markedly from those in which the regulations were originally conceived.

3.2.2 Exploring the Economic Impact of GDPR on Africa

In the context of Africa's dynamic economic environment, particularly with the ambitions of the African Continental Free Trade Agreement (AfCFTA),²⁸⁰ the potential adoption of GDPR-like frameworks in African countries necessitates a context-sensitive analysis. This is because the AfCFTA celebrated as the world's largest free trade area, is designed to expedite the free flow of goods and services across African borders and elevate Africa's position on the global trading stage.²⁸¹ However, while AfCFTA aims to dismantle trade barriers and boost intra-continental trade, particularly in high-value sectors,²⁸² the extraterritorial reach of the GDPR introduces a different set of challenges. Specifically, it imposes significant

²⁷⁸ Enforcement Tracker. (2024). *GDPR fines insights: Trends in enforcement frequency from July 2018 to April 2024*. Available at: <https://www.enforcementtracker.com/?insights>, Accessed 30 April 2024.

²⁷⁹ Yelena Smirnova & Victoriano Travieso-Morales, "Understanding Challenges of GDPR Implementation in Business Enterprises: A Systematic Literature Review" (2024) 66:3 *Intl J of Law & Mgmt* 326, online: ResearchGate <https://www.researchgate.net/publication/377572957>, Accessed 30 April 2024.

²⁸⁰ United Nations Conference on Trade and Development (UNCTAD), "The African Continental Free Trade Area: The Day After the Kigali Summit," Policy Brief No. 67 (May 2018): accessed April 20, 2024, https://unctad.org/system/files/official-document/presspb2018d4_en.pdf.

²⁸¹ *Ibid.*

²⁸² Fagbayibo, Babatunde. "Exploring Legal Imperatives of Regional Integration in Africa." *The Comparative and International Law Journal of Southern Africa* 45, no. 1 (March 2012): 64-76. Published by the Institute of Foreign and Comparative Law.

complexities for African businesses trading with the EU, especially small and medium-sized enterprises (SMEs).²⁸³ Moreover, it is important to clarify that the GDPR's extraterritorial application means that any African SME engaging with EU markets becomes subject to the GDPR, regardless of AfCFTA's objectives. Consequently, the AfCFTA does not provide a buffer from international data protection regulations like the GDPR; rather, African businesses operating globally must navigate both regional trade opportunities and stringent global privacy frameworks. Additionally, African countries, as a regional bloc, have not yet implemented a unified response to GDPR compliance, leaving individual countries to address these challenges on a case-by-case basis.²⁸⁴ This fragmented approach highlights the urgent need for a contextually sensitive privacy and data protection framework that recognizes the specific economic and developmental challenges faced by African SMEs while also enabling them to remain competitive in the global market.

The GDPR's imposition on African businesses trading with the EU can be viewed as a form of regulatory hegemony, where African nations are compelled to align with external legal standards that may not reflect their socio-economic realities. As a result, the economic pressures created by GDPR compliance, particularly for SMEs, highlight the need for African countries to develop privacy and data protection frameworks that are tailored to their unique contexts. A key example of this is Kenya's experience, with a more flexible regulatory stance on privacy has stimulated tech ventures and attracted significant venture capital, illustrating the potential benefits of an adaptable regulatory environment.²⁸⁵ Nevertheless, while AfCFTA provides a framework for economic integration, the GDPR introduces a regulatory burden for African SMEs, especially those engaging in international trade. This is critical because SMEs form the backbone of Africa's economy, accounting for more than 90% of all enterprises and

²⁸³ *Ibid.*

²⁸⁴ *Ibid.*

²⁸⁵ Frizell, Sabina. "How Kenya's New Data Privacy Bill Could Hurt Its Economy." *Council on Foreign Relations*, November 8, 2018. <https://www.cfr.org/blog/howkenyas-new-data-privacy-bill-could-hurt-its-economy> [<https://perma.cc/PM6N-HNRP>] (archived November 12, 2019).

employing about 60% of the workforce.²⁸⁶ However, the GDPR's stringent privacy and data protection standards and significant fines for non-compliance present a disproportionate challenge for these enterprises. For this reason, the costs and complexities involved in adhering to GDPR standards could restrict their growth potential and obstruct broader economic advancement under AfCFTA. Ultimately, this reality points out the need for a regulatory framework that not only protects privacy but also aligns with Africa's broader socio-economic goals, enabling SMEs to thrive in the digital economy without being stifled by external regulatory pressures. While the AfCFTA seeks to foster regional economic integration, African countries must develop a privacy and data protection regime that is both responsive to the continent's specific needs and aligned with global standards. Thus, this requires African policymakers to navigate the complex interplay between economic growth, regional integration, and privacy obligations, ensuring that their regulatory frameworks do not hinder the economic potential of SMEs.

3.3 Legal challenges: A conflict between the GDPR and local Legal frameworks

The introduction of the GDPR into Africa's legal environment introduces significant legal challenges due to the continent's complex and diverse legal systems. Within the African legal systems, a dynamic composition of pluralistic legal traditions coexists, shaped by the continent's diverse colonial legacies and indigenous customs.²⁸⁷ It is noteworthy that Africa's legal framework is a composite of various legal traditions, including indigenous African customary laws, Islamic laws, inherited legal systems from colonial rule, and comprehensive national legislation. This complexity leads to legal conflicts, as the GDPR's standardized and

²⁸⁶ International Trade Centre. *Promoting SME competitiveness in Africa: Data for de-risking investment*. Geneva, September 2018.

²⁸⁷ Kischel, Uwe, and Andrew Hammel, 'The Context of African Law', *Comparative Law* (Oxford, 2019; online edn, Oxford Academic, 17 Apr. 2019), <https://doi.org.proxy.bib.uottawa.ca/10.1093/oso/9780198791355.003.0008>, accessed 4 May 2024.

rigorous approach to data protection often does not align with these pluralistic legal systems. As a result, navigating compliance with the GDPR becomes particularly challenging in Africa.²⁸⁸ Customary law, ingrained in the practices of Africa's ethnic nations, has historically governed the personal affairs of the majority, reflecting the distinct social framework of each community.²⁸⁹ These legal systems, while varied across ethnic lines, share common principles yet are localized to the specificities of each group, emphasizing the deeply embedded nature of customary law within the societal value system. The juxtaposition of these diverse legal traditions with the GDPR presents a unique challenge. The GDPR's standardized and rigorous approach to privacy and data protection stands in stark contrast to the multifaceted legal environment of Africa, where the confluence of customary practices, religious mandates, and colonial legacies form a complex legal framework.²⁹⁰ This plurality, a hallmark of African legal systems, includes the coexistence of customary laws with elements of Islamic Sharia in certain jurisdictions, offering individuals the autonomy to navigate between these legal frameworks based on personal or community affiliation.²⁹¹ For example, in countries like Nigeria, where both customary and Sharia laws govern personal matters,²⁹² aligning with GDPR principles becomes particularly difficult, as these local laws emphasize communal rather than individual privacy rights.

However, the endeavour to align with the GDPR reveals the friction between these pluralistic legal traditions and the GDPR's uniform requirements. The variances in legal foundations and enforcement mechanisms across the African continent not only complicate compliance efforts but also risk exacerbating legal ambiguities.²⁹³ The integration of Sharia

²⁸⁸ Jacques Frémont, "Legal Pluralism, Customary Law and Human Rights in Francophone African Countries" (2009) Victoria U. Wellington L. Rev. 149, 150 et seq.

²⁸⁹ Gordon Woodman, "Legal Pluralism in Africa: The Implications of State Recognition of Customary Laws Illustrated from the Field of Land Law" (2011) 35 Acta Juridica.

²⁹⁰ *Ibid.*

²⁹¹ Kischel and Hammel, *supra* note 287.

²⁹² Miles, John. "Customary and Islamic Law and Its Development in Africa." Law for Development Review, African Development Bank, 2007, pp. 99-125.

²⁹³ Kischel and Hammel, *supra* note 287.

law into the national legal frameworks of some African countries, contrasted with the discretion that allows others to choose between customary and Sharia laws, illustrates the complexities inherent in reconciling local legal norms with the GDPR standards. This intricate legal plurality, while reflective of Africa's rich cultural and historical tapestry, poses significant challenges in harmonizing with the GDPR's singular approach and mandates.

Subsequently, in many African countries, privacy and data protection laws are treated synonymously, with the safeguarding of personal data seen as an inherent part of the right to privacy.²⁹⁴ This approach, while progressive, diverges from the GDPR's separation of data protection and privacy. For instance, Uganda's Data Protection and Privacy Act, 2019 integrates these concepts, making compliance with GDPR's data protection-specific mandates more complex in the African context. The Act's preamble articulates the intent to:

...protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processors, and data controllers; to regulate the use or disclosure of personal information; and for related matters.²⁹⁵

While Uganda's legal stance may not represent the entire African continent, it serves as a key illustration of a common African viewpoint: privacy laws are often synonymous with data protection legislation, rooted in the constitutional right to privacy. This perspective treats the safeguarding of personal data as an inherent aspect of privacy rights. The emphasis on data protection as a definitive expression of privacy rights is a significant advancement for the African region, yet it also signals a unique interpretation.

Expanding on this foundation, Africa's regulatory environment features a complex array of legal mechanisms, from stringent statutes to more adaptable, non-binding guidelines. The role of soft laws is particularly notable for their adaptability and capacity to foster

²⁹⁴ Access Now, "Strengthening Data Protection in Africa: Key Issues for Implementation" (Access Now, 2024), by Bridget Andere and Megan Kathure, accessed January 2024, <https://www.accessnow.org/wp-content/uploads/2024/01/Strengthening-data-protection-in-Africa-key-issues-for-implementation-updated.pdf>.

²⁹⁵ Uganda, The Data Protection and Privacy Act, 2019, Preamble.

consensus, crucial in societies that prioritize communal decision-making.²⁹⁶ This approach is evident in initiatives like the Model Laws of the Southern African Development Community (SADC) and the Economic Community of Central African States (ECCAS),²⁹⁷ which provide comprehensive guidelines and encourage collaboration among member states. Yet, crafting a unified approach to privacy and data protection across the continent poses difficulties. The consideration of whether to employ uniform regulations akin to the EU's GDPR or to adopt variable, risk-based strategies highlights the dilemma of practical enforcement in Africa's varied legal environment.

Contrasting with the EU's GDPR, which establishes a cohesive data protection regime across its member states, African countries operate under their unique national legislations, crafted to address the particular privacy and data protection challenges within their jurisdictions. An examination of statutes such as the Protection of Personal Information Act (POPIA) of 2013 from South Africa, the Data Protection Regulation (NDPR) of 2019 from Nigeria, and the Data Protection Act (DPA) of 2019 from Kenya reveals both similarities and discrepancies with the GDPR. These legislations are selected for analysis due to their prominence and the insight they offer into Africa's approach to data protection. While not exhaustive of the continent's legal framework, these examples serve to illuminate the variances in how African countries conceptualize and implement data protection policies, providing a window into the broader challenges and adaptations evident across the continent's regulatory environments. Specifically, South Africa's POPIA, which governs the processing of personal information, aligns with the GDPR on several core principles, including transparency, consent, and the security of data.²⁹⁸ Nonetheless, differences are

²⁹⁶ Patricia Boshe, Moritz Hennemann, and Ricarda von Meding, "African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward" (2022) 3(2) Global Privacy Law Review.

²⁹⁷ Southern Africa Development Community (SADC), Economic Community of Central African States (ECCAS).

²⁹⁸ OneTrust DataGuidance, *Comparing Privacy Laws: GDPR v. POPIA*, online: https://www.dataguidance.com/sites/default/files/onetrustdataguidance_comparingprivacylaws_gdprvpopia.pdf.

apparent, such as POPIA's absence of guidelines on pseudonymized data processing, higher age of consent for children's data, and less detailed directions on impact assessments.²⁹⁹ Moreover, unlike the GDPR, POPIA does not feature a right to data portability.³⁰⁰ Nigeria's NDPR and Kenya's DPA, while reflecting GDPR's emphasis on consent, rights of the data subject, and data security, also exhibit notable differences.³⁰¹ Issues such as the handling of pseudonymized data, data processors' record-keeping duties, and the protocol for data breach notifications vary. Although both the NDPR and DPA recognize the right to data portability, their implementation and scope diverge from the GDPR model.³⁰²

Moving beyond these individual regulations, the broader scope and varied enforcement mechanisms further highlight the differences between African data protection laws and the GDPR. African regulations typically have jurisdiction only within their territories, contrasting with the GDPR's extraterritorial applicability. Enforcement of the GDPR is centralized under the European Data Protection Board (EDPB), an independent body that ensures uniform application of the GDPR across the EEA.³⁰³ It comprises the heads of national data protection authorities and the European Data Protection Supervisor, collaborating to enforce data protection law, including through binding decisions in cross-border disputes.³⁰⁴ This cohesive framework, supported by a Secretariat based in Brussels, facilitates a consistent approach to data protection across the EEA.³⁰⁵

African countries each have their distinct mechanisms for enforcing data protection laws, which leads to considerable variation across the continent in both the methods used and the severity of penalties imposed. This results in a fragmented enforcement regime, where

²⁹⁹ *Ibid.*

³⁰⁰ *Ibid.*

³⁰¹ Ana Mishova, "GDPR and Data Protection Laws in Africa: A Comparison" (29 November 2023) online: GDPR Local <https://gdprlocal.com/gdpr-and-data-protection-laws-in-africa-a-comparison/>.

³⁰² *Ibid.*

³⁰³ European Data Protection Board, *The European Data Protection Board* (last updated 6 April 2022), online: European Data Protection Board https://www.edpb.europa.eu/edpb_en.

³⁰⁴ *Ibid.*

³⁰⁵ *Ibid.*

penalties and compliance requirements vary significantly across the continent. For example, while Kenya has issued the highest number of penalties, the total value of these fines is significantly lower than those imposed in South Africa, Nigeria, and Angola.³⁰⁶ In Nigeria, the data protection authority levied fines against banks, telecommunications firms, and digital lending institutions for breaches related to data privacy.³⁰⁷ However, the specifics of these entities were not disclosed. South Africa's Information Regulator (IR) marked a notable enforcement action by imposing a ZAR 5 million fine (approximately \$279,000) on the Department of Justice and Constitutional Development for failing to renew licenses for critical cybersecurity components such as anti-virus, security information and event management (SIEM), and intrusion detection systems.³⁰⁸ This was the only penalty reported against a public body in the region for violations of the Protection of Personal Information Act (POPIA).³⁰⁹ Additionally, the Information Regulator issued an enforcement notice to Dis-Chem due to a data breach stemming from a vendor incident on September 6, 2023, marking another significant enforcement action related to POPIA violations.³¹⁰ In Angola, the National Data Protection Authority fined Africell \$150,000 for processing customers' data without prior authorization from the NDPA,³¹¹ highlighting the varying enforcement landscape across Africa due to the absence of a pan-African equivalent to the EDPB. Such variations clarify the challenges and strategic considerations necessary to navigate Africa's diverse legal landscape of privacy and data protection. They highlight the importance of understanding the

³⁰⁶ Africa Privacy Report. *Africa Privacy Report 2023-2024*. Lawyers Hub, 2023.

³⁰⁷ *Ibid*.

³⁰⁸ Li, R. (2023) South African government fined for data breach, ALB. Available at: <https://www.africanlawbusiness.com/news/19143-southafrican-government-fined-for-data-breach> (Accessed: 1 May 2024).

³⁰⁹ *Ibid*

³¹⁰ Ahmore Burger-Smidt. "Enforcement Notice Issued to Dis-Chem Due to Contravention of POPIA." Werksmans Attorneys, September 18, 2023. <https://www.werksmans.com/legal-updates-and-opinions/enforcement-notice-issued-to-dis-chem-due-to-contravention-of-popia>.

³¹¹ Sheik, S. (2023) Data Protection Fines in Africa, Michalsons.com. Available at: <https://www.michalsons.com/blog/data-protection-fines-in-africa/64822> (Accessed: 1 May 2024).

localized enforcement paradigms, emphasizing the complex balance between adhering to local regulations and engaging in the global digital economy.

Nevertheless, efforts to adopt GDPR-like principles in African laws do not ensure mutual compliance; adherence to laws such as POPIA, NDPR, or DPA does not automatically equate to GDPR compliance, and the reverse is also true. Given the complexities of aligning Africa's pluralistic legal systems with GDPR, it may be worth considering an approach similar to the Canadian or US model, where compliance with GDPR-like regulations is limited to specific sectors, such as trade and commerce.³¹² This would allow African countries to balance privacy concerns with the need to foster economic growth, particularly for SMEs that could be disproportionately affected by stringent GDPR requirements. For instance, South Africa's POPIA aligns with GDPR on many core principles but lacks provisions for data portability and pseudonymization.³¹³ Therefore, while adhering to African data protection laws may smooth the path toward GDPR compliance, significant disparities remain that complicate the overall compliance process. This understanding forms the basis for Chapter 4, which will explore Africa's legal frameworks regarding privacy and data protection. This section serves as an introduction, establishing the foundation for a more comprehensive analysis in the forthcoming chapter.

3.4 Cultural Distinctions: GDPR Adoption Challenges in Africa

The influence of culture on the formulation and adoption of privacy and data protection laws cannot be overstated. Culture, a complex tapestry of shared beliefs, practices, values, and norms, deeply influences societal behaviours and perspectives, guiding collective

³¹² Grynwajc, Stephan. "Privacy at the Crossroads: A Comparative Analysis of Regulation in the U.S., the EU and Canada." *The Transatlantic Lawyer*, 2022, online: <https://www.transatlantic-lawyer.com/privacy-laws-focus-on-a-transatlantic-perspective/>, accessed October 15, 2024.

³¹³ OneTrust DataGuidance. "Comparing Privacy Laws: GDPR v. POPIA." OneTrust DataGuidance, 2021.

identities and ways of life.³¹⁴ In the domain of privacy and data protection, culture shapes the foundational norms, values, and beliefs that drive a country's regulatory framework. The relationship between cultural values and privacy and data protection laws is marked by varied perceptions and practices across the world, reflecting the unique interplay between societal norms and legal structures.³¹⁵ Central to understanding this dynamic is the African cultural philosophy, often encapsulated in the philosophy of *Ubuntu*, which translates to "*I am because we are*."³¹⁶ This principle emphasizes the essence of communal existence, valuing the collective over the individual and highlighting the significance of communal bonds and kinship. When contrasting African and Western societal structures, distinct cultural norms around privacy and data protection emerge. African societies are characterized by their communal orientation, where the extended family and broader kinship networks play a crucial role in daily life,³¹⁷ contrasting with the more individualistic nuclear family model prevalent in Western contexts.³¹⁸ In African communities, the extended family's reach and influence extend far beyond the immediate household, creating a network of interconnectedness and shared communal identity.³¹⁹

This communal mindset shapes distinct perspectives on privacy and data protection, where principles of group cohesion, uniformity, and collective identity predominate.³²⁰ Unlike Western individualistic approaches that emphasize personal autonomy and control over personal information,³²¹ African cultures prize communal harmony, interdependence,

³¹⁴ Timileyin, Oluwatobi. "Unveiling the Tapestry: Exploring the Intersections of Culture and Society." *Medium*. <https://medium.com/@timileyinoluwatobi1995/unveiling-the-tapestry-exploring-the-intersections-of-culture-and-society-1c187d1e3cdf>.

³¹⁵ *Ibid.*

³¹⁶ In African scholarship, Ubuntu is understood as an African philosophy emphasizing collectivist human relationships and assistance in everyday life, whereby individuals are subject to communal considerations. While primarily developed in South African scholarship, the concept also resonates in other African societies.

³¹⁷ Cobbah, Josiah A. M. "African Values and the Human Rights Debate: An African Perspective." *Human Rights Quarterly* 9, no. 3 (August 1987): 309-331. Published by The Johns Hopkins University Press.

³¹⁸ *Ibid.*

³¹⁹ *Ibid.*

³²⁰ *Ibid.*

³²¹ *Ibid.*

and collective responsibility.³²² These values inform a communal approach to privacy and data protection, where the well-being of the community often takes precedence over individual preferences.³²³ In African societies, the extended family structure significantly influences the allocation of social roles, with a system that supports reproduction, economic sustenance, and socialization within a collective framework.³²⁴ The conception of kinship within these societies also differs markedly from Western notions, with a less strict distinction between various familial roles. For example, in most African cultures, such as among the Banyoro of Uganda, the terminology for familial relationships is not sharply delineated; all older female relatives might be referred to as mother, and cousins are viewed similarly to siblings, reflecting the societal preference for matrilineal or patrilineal lineage.³²⁵ These cultural nuances highlight the rich tapestry of social dynamics that influence attitudes toward privacy and data protection in African contexts. The fluidity of kinship relations and the emphasis on collective over individual values present unique considerations for the development and implementation of privacy regulations, underlining the need for a context-sensitive understanding of cultural impacts on privacy norms and legislation.

The designations employed within African family structures are deeply rooted in the societal values, norms, and roles traditionally expected of kin.³²⁶ These designations serve to formalize the social roles within the family, clearly delineating the responsibilities and privileges of each member.³²⁷ In such settings, rights and duties are reciprocal, emphasizing the web of interdependence that is central to African family life and shaping how members interact and fulfill obligations to one another. Reflecting on the perspectives shared by Niara Sudarkasa, it is clear that the complexities seen in larger family units within European

³²² *Ibid*

³²³ *Ibid.*

³²⁴ *Ibid.*

³²⁵ Summary: Fur. *eHRAF World Cultures*. <https://ehrafworldcultures.yale.edu/cultures/fk11/summary>.

³²⁶ *Ibid.*

³²⁷ Cobbah, *supra* note 317.

contexts do not hold the same connotations in African societies.³²⁸ The African extended family is a fundamental societal unit, deeply integrated into cultural practices, and it warrants consideration of its broader implications rather than being viewed through a problematizing lens.³²⁹ Analyzing these family dynamics with a Western perspective focused on individualism may conceal the true nature of the communal structures inherent in African societies.

African families maintain their unity through explicit social codes that guide interactions within the kinship group.³³⁰ What might be seen as burdensome from a Western viewpoint are accepted and indeed valued practices within African communities, with their worth recognized in the reciprocity they foster. Sudarkasa brings to light four pillars that are central to African family life: respect, restraint, responsibility, and reciprocity.³³¹ Respect is a cornerstone within African familial and societal relations, and it is particularly expressed through the deference shown to elders.³³² African communities, while communal, also respect the hierarchy that places elders at the top. This respect is instilled from childhood and is evident in the reverence and recognition given to those with seniority, which, over time, every individual can attain based on age and wisdom rather than on other status indicators.³³³ Restraint is another guiding principle, reinforcing the communal ethos by acknowledging that personal freedoms are not unfettered and must be balanced against the community's welfare.³³⁴ This tenet manifests in all facets of life, dictating that the collective good often supersedes individual desires, which can be seen in the way families support each other financially and emotionally.³³⁵ In African communities, responsibility is attributed to a wider

³²⁸ Sudarkasa, Niara. "African and Afro-American Family Structure: A Comparison." *Black Scholar* 11. (November/December 1980): 44. Cited in Cobbah, supra note 317.

³²⁹ *Ibid.*

³³⁰ *Ibid.*

³³¹ *Ibid.*

³³² *Ibid.*

³³³ *Ibid.*

³³⁴ *Ibid.*

³³⁵ *Ibid.*

scope than in Western societies. The expansive family networks provide not only support but also entail significant duties for each member. This involves a commitment to contribute to the family's overall well-being and the upholding of family traditions and responsibilities.³³⁶ Lastly, reciprocity is woven into the tradition of African social life, where generosity is not just encouraged but expected to be returned. This reciprocal giving forms a cycle of support that spans generations, ensuring that acts of kindness are paid forward and reinforcing the bonds of kinship that are pivotal to African communities.³³⁷

Drawing from this understanding, African communalism offers a distinct worldview, emphasizing the collective over the individual, where personal interests are interwoven with the community's well-being. This philosophy, deeply rooted in the social culture of African societies, advocates for conflict resolution through consensus and shared responsibility, presenting a contrast to cultures that prioritize individual autonomy.³³⁸ Within this framework, individuals are seen as integral parts of a larger continuum, their identities connected to both ancestral heritage and future generations, thus offering a narrative that significantly diverges from the individualistic focus prevalent in European thought.³³⁹ In African contexts, privacy and data protection are often understood through a community-oriented lens rather than an individual-centric one. This perspective is rooted in a cultural framework that values communal well-being and collective support over individual autonomy.³⁴⁰ Within this paradigm, the concept of human dignity is interpreted through communal relationships and shared responsibilities, differing markedly from the individual rights-based approach prevalent in Western societies. These foundational cultural values profoundly shape the African approach to privacy and data protection, steering it towards

³³⁶ Herbert J. Foster, "African Patterns in the Afro-American Family," (1983) 14 J Black Stud 210, cited in Cobbah, *supra* note 317.

³³⁷ *Ibid.*

³³⁸ Cobbah, *supra* note 317.

³³⁹ *Ibid.*

³⁴⁰ *Ibid.*

collective interests and communal rights. This collective viewpoint offers a distinct interpretation of human dignity and privacy, emphasizing the interdependence of individuals within the broader social framework.

Moreover, the GDPR is fundamentally rooted in an individualistic framework, one that embodies Western legal traditions more than communal ones. It accentuates the individual's rights and autonomy in data protection rather than an individual's responsibilities towards the community, which is often the focal point in African societies. This emphasis on the individual aligns with a Western viewpoint that values personal liberty and privacy. For example, the GDPR enshrines several rights that illustrate this individual-centric perspective. The right to access³⁴¹ empowers individuals to inquire and gain access to their data held by data controllers, exemplifying the principle of personal control over one's information. The right to rectification³⁴² allows individuals to amend their data, ensuring they have authority over their digital representations. Furthermore, the right to erasure, also known as the right to be forgotten,³⁴³ entitles individuals to have their data erased, prioritizing their right to privacy over potential competing interests, such as the data controller's need to retain that data. The right to data portability³⁴⁴ facilitates an individual's ability to transfer their data between platforms, reinforcing the individual's agency and empowerment in the digital environment. The GDPR's stance on consent³⁴⁵ highlights the importance of individual agreement in data processing activities, requiring data controllers to secure explicit and affirmative consent, thereby spotlighting the right to personal decision-making in data-related matters.

In integrating these rights, the GDPR distinctly privileges individual autonomy and control over personal data, mirroring the Western value system where the individual's preferences and rights are paramount. For effective implementation in African countries, it is

³⁴¹ GDPR, *Article 15*.

³⁴² GDPR, *Article 16*.

³⁴³ GDPR, *Article 17*.

³⁴⁴ GDPR, *Article 20*.

³⁴⁵ GDPR, *Article 7*.

necessary to consider how these rights can coexist with the communal responsibilities and collective values deeply ingrained in African cultures. The challenge lies in reconciling the GDPR's individualistic approach with the communal principles central to the African worldview. African national laws, however, attempt to reflect this communal ethos. For instance, South Africa's POPIA not only emphasizes data subject rights but also promotes data processing that benefits broader societal and communal needs.³⁴⁶ Similarly, Nigeria's NDPR includes provisions that protect community interests by regulating digital data exchanges in ways that align with traditional societal norms.³⁴⁷ Kenya's Data Protection Act³⁴⁸ and Uganda's Data Protection and Privacy Act³⁴⁹ embody a hybrid approach, where individual rights are acknowledged, but collective welfare is considered when dealing with personal data at the community level. These national frameworks, though influenced by global data protection standards, illustrate attempts to balance individual data rights with Africa's strong communal values, ensuring that privacy protection operates in a way that aligns with the broader societal context.

3.5 Financial and Technological Roadblocks to GDPR Compliance in Africa

Building on the previous discussion regarding the cultural nuances influencing privacy and data protection laws in Africa, it becomes evident that achieving GDPR compliance in the region is not merely a matter of legal adaptation but also a formidable economic, technological, social and cultural endeavour. Exploring the economic and technological barriers that African countries face in the pursuit of GDPR compliance reveals

³⁴⁶ OneTrust DataGuidance. "Comparing Privacy Laws: GDPR v. POPIA." OneTrust DataGuidance, 2021; South Africa, *Protection of Personal Information Act* 4 of 2013, ss 1, 19.

³⁴⁷ National Information Technology Development Agency (NITDA), *Nigeria Data Protection Regulation 2019: Implementation Framework* (2020); Nigeria, *Data Protection Act*, 2023, ss 2(2)(a), 24(3), 44.

³⁴⁸ Kenya, *Data Protection Act*, No 24 of 2019, ss 25(d), 30(1)(d)(iii), 31(1).

³⁴⁹ Uganda, *Data Protection and Privacy Act*, No 9 of 2019, ss 3(b), 7(1)(d), 18(1)(d); Uganda, *Data Protection and Privacy Regulations*, 2021, regs 6(1)(d), 8(1)(c), 10(1)(a).

the importance of understanding the continent's technological capabilities and economic framework. This analysis brings attention to the diverse challenges encountered as African countries aim to satisfy the demanding privacy and data protection standards mandated by the GDPR, providing a clearer view of the challenges of adhering to the GDPR regulatory standards within the distinctive African environment.

Moreover, the process of achieving GDPR compliance has unveiled significant financial challenges, particularly pronounced in the context of Africa's technological infrastructure. The gap between the infrastructural capabilities of African countries and those of European countries presents a significant obstacle to meeting the GDPR's stringent data protection requirements.³⁵⁰ The financial impact of adhering to these standards poses a considerable challenge to the technological and economic growth of the continent. The imposition of substantial fines on major corporations for GDPR violations underlines the financial implications of the regulation.³⁵¹ The profound impact on SMEs, which are crucial to Africa's economy, more precisely depicts the significant economic implications for African countries. These businesses face considerable financial pressure in their efforts to comply with the GDPR, a situation exacerbated by the need for significant investments in data protection, cybersecurity technologies, and compliance processes.³⁵²

A critical analysis of GDPR compliance costs reveals distinct financial pressures across various sectors of the economy. These burdens are especially pronounced in industries heavily reliant on the processing and safeguarding of personal data. The banking sector, for instance, incurs significantly higher compliance costs due to its stringent regulatory environment and the volume of sensitive data handled.³⁵³ Similarly, the technology and

³⁵⁰ Cara Mannion, "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets," *Vanderbilt Journal of Transnational Law* 53, no. 2 (March 2020).

³⁵¹ Ibid.

³⁵² Ibid.

³⁵³ Sia Partners, "Average Estimated GDPR Costs for FTSE100 Companies in the United Kingdom in 2018, by Sector" (May 2018), online: Sia Partners <https://en.finance.sia-partners.com>, Accessed 30 April 2024.

telecom sectors face steep expenditures as they navigate complex data ecosystems and rapidly evolving regulatory expectations.³⁵⁴ Conversely, sectors such as industrial goods and services exhibit comparatively lower compliance costs, reflecting the lesser degree of dependency on personal data.³⁵⁵ This disparity highlights a broader economic reality: industries with robust resources and global reach are better positioned to meet GDPR obligations, whereas smaller or less data-intensive sectors may experience compliance as a less burdensome, albeit still significant, requirement. These sectoral differences highlight the uneven financial landscape of GDPR enforcement. Larger corporations, particularly in the banking and technology sectors, can often absorb these costs within their extensive operational budgets. However, smaller firms or those in less affluent regions may struggle to meet compliance standards without compromising their financial stability or growth potential. This uneven distribution of regulatory costs risks perpetuating existing economic hierarchies, where compliance becomes an additional barrier for less resource-intensive industries or regions with limited economic capacity. This dynamic invites a reflection on the broader implications of one-size-fits-all regulatory frameworks in diverse economic contexts. The uniform application of GDPR across sectors and regions, despite significant variations in financial and operational capacities, emphasizes the need for a more refined understanding of how global regulatory standards intersect with local economic realities.

The expenses involved in achieving and maintaining GDPR compliance are varied, depending on factors such as the size of the organization, the volume and sensitivity of the personal data processed, and the cybersecurity risks faced.³⁵⁶ For African companies, especially SMEs, the cost of compliance extends beyond direct financial investment to include thorough risk assessments, the strengthening of data security measures, ongoing

³⁵⁴ *Ibid.*

³⁵⁵ *Ibid.*

³⁵⁶ Johnson, Garrett A. "Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond." *Questrom School of Business, Boston University*, June 16, 2023.

compliance audits, and the continuous refinement of data management practices.³⁵⁷ These efforts are critical not only to minimize the risk of data breaches but also to protect against the severe financial and reputational repercussions of GDPR infractions. Furthermore, aligning with GDPR standards often requires a significant overhaul of existing technological frameworks and business operations, potentially involving the adoption of cutting-edge cybersecurity solutions, the establishment of secure data management systems, and comprehensive training for staff in privacy and data protection protocols.³⁵⁸ The aggregate expense of these initiatives, particularly for organizations dealing with sensitive or vast amounts of data, demands a deliberate allocation of resources dedicated to data protection strategies.³⁵⁹

Furthermore, the journey towards GDPR compliance in Africa encounters significant obstacles due to limitations in technological infrastructure.³⁶⁰ This issue is common across African countries despite their cultural and economic diversity; it hampers the consistent adoption of GDPR standards and threatens the innovative growth and digital economy expansion that some African countries, like Kenya, have experienced under less stringent data privacy laws.³⁶¹ The introduction of the GDPR's stringent standards risks diminishing the competitive advantages these countries have enjoyed, potentially stifling the spirit of innovation that has characterized Africa's digital progress. SMEs, pivotal to Africa's economy, are particularly vulnerable.³⁶² The transition to rigorous privacy and data protection

³⁵⁷ Mannion, *Supra* note, 349.

³⁵⁸ Johnson, *supra* note, 356.

³⁵⁹ *Ibid.*

³⁶⁰ Mannion, *Supra* note, 350.

³⁶¹ Frizell, Sabina. "How Kenya's New Data Privacy Bill Could Hurt Its Economy." *Council on Foreign Relations* (November 8, 2018). <https://www.cfr.org/blog/how-kenyas-new-data-privacy-bill-could-hurt-its-economy>, Cited in: Mannion, Cara. "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets." *Vanderbilt Journal of Transnational Law* 53, no. 2 (March 2020): 698.

³⁶² Mannion, *Supra* note, 350.

standards limits operational flexibility and increases the likelihood of non-compliant practices due to the cost of compliance and the risk of enforcement.³⁶³

Moreover, the broader implications of GDPR non-compliance extend beyond immediate financial or reputational damages. A failure to comply can erode investor confidence and lead to investment losses.³⁶⁴ Research by PricewaterhouseCoopers indicates that companies emphasizing GDPR compliance are positioning themselves more attractively in the market, suggesting that GDPR adherence is becoming a crucial factor for investors and consumers alike.³⁶⁵ This development may disadvantage companies that lag in compliance, potentially leading to reduced customer trust and loss of clientele.

Enforcement of comprehensive privacy and data protection laws that align with GDPR principles represents another pivotal challenge. Many African countries are grappling with the need for stable and effective judicial systems capable of upholding such legislation.³⁶⁶ The absence of robust enforcement capabilities is a significant barrier to realizing the full benefits of GDPR-aligned data privacy laws. It renders the legislative advances potentially superficial if individuals lack a reliable avenue for redress in instances where their data rights are infringed.³⁶⁷ For African countries, the task of achieving GDPR compliance encompasses not only the legislative process of enacting aligned laws and regulations but also the establishment of enforcement mechanisms that ensure these laws are more than just token gestures.³⁶⁸ The presence or absence of such mechanisms can profoundly influence the success of GDPR implementation efforts across the continent.

³⁶³ *Ibid.*

³⁶⁴ *Ibid.*

³⁶⁵ PwC. "A Privacy Reset — From Compliance to Trust-Building." PwC, [accessed May 1, 2024].

<https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/privacy-reset.html>.

³⁶⁶ Mannion, *Supra* note, 350.

³⁶⁷ *Ibid.*

³⁶⁸ Makulilo, Alex B. "The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius." *The International Journal of Human Rights* 25, no. 1 (2021): 117-146.

Consequently, the EU employs a rigorous set of criteria to appraise the adequacy of a non-EU country's data privacy legislation regarding the GDPR. This assessment encompasses not only the legal texts but also the country's ability to implement and enforce the legislation effectively, alongside a demonstrated adherence to the rule of law.³⁶⁹ However, various African countries encounter significant hurdles in meeting these EU benchmarks, often reflected in their performance on global indices such as the World Bank's Rule of Law Index, which measures the public's confidence in the judiciary, the enforcement of rights, and general compliance with laws.³⁷⁰ Even in instances where African countries have managed to craft legislation that is ostensibly aligned with GDPR principles, the practical enforcement of these laws is frequently compromised by judicial systems that are beleaguered by inefficiency, delays, and corruption.³⁷¹ Such systemic flaws undermine public trust and discourage individuals from pursuing legal recourse for privacy and data protection violations.³⁷²

Additionally, the establishment and empowerment of independent data protection agencies, critical for the enforcement of privacy laws, remain an unfulfilled goal in many African countries.³⁷³ Where these agencies do exist, their operational efficacy is often undermined by a lack of independence from government influence, as discussed later on in the chapter from the different African country cases. Moreover, the establishment of rigorous data protection frameworks often competes with other pressing national concerns such as corruption and public health crises.³⁷⁴ In environments where basic needs such as access to

³⁶⁹ European Data Protection Board, *supra* note 303.

³⁷⁰ Rule of Law Index, WORLD BANK, <https://perma.cc/GJF7-ZEWA>] (archived Nov. 12, 2019) (the Rule of Law Index is being used as a proxy for evaluating the efficacy of judicial institutions in African countries).

³⁷¹ Paradigm Initiative and Olumide Babalola LP. *Data Protection Authorities in Africa: A Report on the Establishment, Independence, Impartiality and Efficiency of Data Protection Supervisory Authorities in the Two Decades of their Existence on the Continent*. Lagos, Nigeria: Paradigm Initiative; July 2021.

³⁷² *Ibid.*

³⁷³ *Ibid.*

³⁷⁴ *Ibid.*

clean water and secure housing remain unmet, data protection may not emerge as a legislative or administrative priority.³⁷⁵

Therefore, the allocation of limited resources to more immediate socio-economic challenges may take precedence, leaving the development of data protection infrastructures as a secondary consideration.³⁷⁶ This complex prioritization reflects the multifaceted socio-economic realities that influence privacy and data protection efforts in African settings, illustrating the need for tailored approaches that acknowledge and address the specific conditions and constraints of each country.

3.6 Institutional Challenges in Upholding GDPR-Inspired Legislation in Africa

Within this context, the structure of governance within Africa is a multilayered array that incorporates continental, regional, and national institutions, each playing a pivotal role in policy development, application, and adjudication. Nationally, constitutions lay the cornerstone for governance, encapsulating the distinctive features and cultural nuances of each country.³⁷⁷ Within these constitutions often lie embedded tenets of privacy and data protection, demonstrating a theoretical underpinning for the protection of these rights. At a regional level, Regional Economic Communities (RECs) act as vital conduits for the advancement of governance aims, playing a significant part in spurring regional growth and fostering integration.³⁷⁸ These RECs, formally recognized by the African Union (AU), synergize with Regional Mechanisms to ensure consistency with overarching continental aspirations.³⁷⁹ Among these, the AU officially designates eight RECs: the Arab Maghreb Union (UMA), the Common Market for Eastern and Southern Africa (COMESA), the

³⁷⁵ *Ibid.*

³⁷⁶ *Ibid.*

³⁷⁷ Bryant, Justin. "Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights." *Stanford Technology Law Review* 24, no. 2 (2021): 389-446.

³⁷⁸ African Union. "Agenda 2063." *African Union*. <https://au.int/en/agenda2063/overview> (accessed May 8, 2024).

³⁷⁹ *Ibid.*

Community of Sahel-Saharan States (CEN-SAD), the East African Community (EAC), the Economic Community of Central African States (ECCAS), the Economic Community of West African States (ECOWAS), the Intergovernmental Authority on Development (IGAD), and the Southern African Development Community (SADC).³⁸⁰ Collectively, these entities strive for governance harmonization and regional solidarity, echoing the AU's continental objectives.

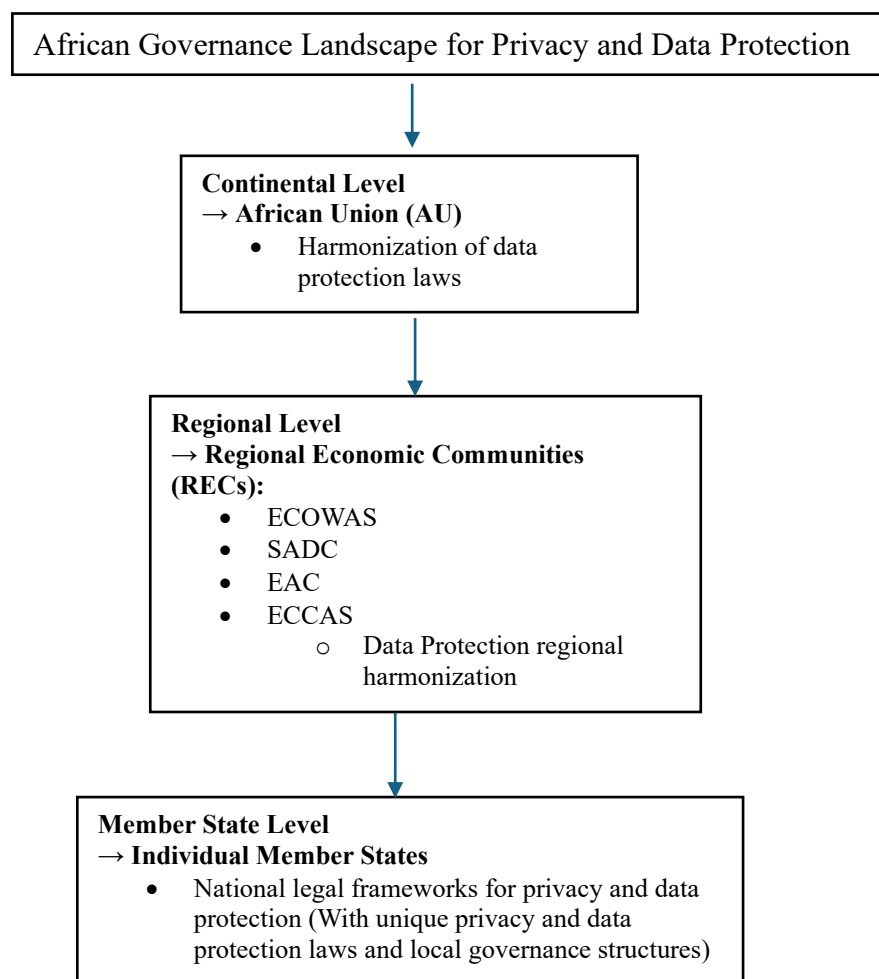


Figure 1: This structure illustrates how governance operates at different levels within Africa, from the continental level led by the African Union to the regional level with Regional Economic Communities (RECs) and down to the Member State level with individual country constitutions. Each level plays a distinct role in policy formulation, coordination, and implementation, contributing to broader objectives of regional integration and development.

³⁸⁰ *Ibid.*

At the forefront, the AU itself is structured with a complex arrangement of governing bodies, encompassing the Assembly of the Union, the Executive Council, the Peace and Security Council, the Pan-African Parliament, and legal structures such as the AU Commission and the Permanent Representatives Committee, among others.³⁸¹ These bodies, along with Specialized Technical Committees, the Economic, Social and Cultural Council, and the African Committee on the Rights and Welfare of the Child, form the institutional bedrock of the AU's governance.³⁸² While these institutions reflect a robust architectural design for governance, operational challenges persist, particularly in aligning and enforcing GDPR-inspired data protection legislation.³⁸³ The complexities inherent to this multilayered governance result in fragmented approaches to policy enforcement, and the variation in institutional capacities and legal frameworks across the continent thus inconsistent applications of privacy and data protection laws.³⁸⁴ This fragmentation is exacerbated by the potential lack of coordination and resource allocation necessary to support effective enforcement mechanisms, leaving the commitment to privacy and data protection variably realized across the continent.³⁸⁵

Within the African structure, local governance serves as the foundational layer of public administration, bridging the gap between state authorities and the communities they serve.³⁸⁶ These grassroots entities, whether termed assemblies, councils, or municipalities, exhibit core structural and functional consistencies across linguistic and regional variations.³⁸⁷ Nonetheless, the endeavour to institutionalize the GDPR in Africa encounters significant hurdles due to the continent's diverse institutional and legal frameworks. A key

³⁸¹ *Ibid.*

³⁸² *Ibid.*

³⁸³ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

³⁸⁴ *Ibid.*

³⁸⁵ *Ibid.*

³⁸⁶ African Peer Review Mechanism. *Africa Governance Report: Promoting African Union Shared Values*. African Peer Review Mechanism, 2021.

³⁸⁷ *Ibid.*

obstacle to the seamless integration of GDPR standards across the continent is the disparity in privacy and data protection laws among member states within various RECs.³⁸⁸ These differences in legal interpretations and enforcement practices complicate the harmonization process, posing a barrier to the cohesive adoption of GDPR-aligned regulations. As of April 2024, a survey of the legal framework across Africa reveals that only thirty-six out of fifty-five African countries have enacted data protection laws and/or regulations.³⁸⁹ Furthermore, nineteen countries have signed the AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention), with fifteen ratifications.³⁹⁰ This patchwork of legal frameworks highlights the challenge of achieving a unified standard for data protection across the continent. This discrepancy in legal standards is pivotal, as it not only impedes the uniform application of data protection principles but also reflects the broader challenge of legislative alignment within diverse governance contexts. The presence of comprehensive legal frameworks in some African countries juxtaposed against the absence in others, coupled with varying levels of enforcement capability, illustrates the fragmented approach to privacy and data protection across the continent.³⁹¹

The endeavour to align the GDPR has led several African countries to reform their legislative frameworks. Nonetheless, the process of adopting laws based on European models presents unique challenges in their application within the distinct socio-political and economic landscapes of Africa. While some countries are in the draft stages of their data protection laws, others have yet to initiate legislative reforms in this domain.³⁹² A notable challenge arises from the direct transplantation of European legal provisions into African statutes without a corresponding enforcement strategy tailored to the local context.

³⁸⁸ Bryant, Justin, *supra* note 377.

³⁸⁹ Lawyers Hub. *Africa Privacy Report 2023/2024: A Review of Policy Trends and Digital Frontiers in Africa's Data Protection Landscape*. Nairobi, Kenya: Lawyers Hub, 2023.

³⁹⁰ African Union. *African Union Convention on Cyber Security and Personal Data Protection*. Adopted June 27, 2014. <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

³⁹¹ Lawyers Hub, *supra* note 389.

³⁹² *Ibid.*

Recognizing these foundational challenges, the following detailed analysis focuses on regional variations and the practical limitations of transplanting the GDPR framework into national laws across Africa, highlighting the persistent difficulties faced in striving for GDPR compliance within diverse regional contexts.

3.7 Challenges in Harmonizing Data Protection Legislation Across Africa: A Review of Regional Efforts and Implementation Hurdles

This section critically evaluates the efforts by various African countries to harmonize their data protection legislation with the GDPR. Historically influenced by the 1995 EU Directive on Data Protection, which the GDPR later superseded, African countries continue to face challenges integrating GDPR standards into their unique socio-political and economic contexts.³⁹³ The direct importation of European legal frameworks without adapting enforcement strategies to local realities often undermines the efficacy of these laws. Furthermore, the establishment and empowerment of independent data protection agencies, essential for enforcing privacy and data protection laws, have not been fully achieved. Where such agencies exist, their effectiveness is frequently compromised by insufficient autonomy from governmental influence.³⁹⁴ Particularly illustrative is the case of Ghana, which has been proactive in aligning its privacy and data protection standards with global norms and actively participating in regional efforts under ECOWAS. Ghana was among the first countries to sign the Malabo Convention in 2014,³⁹⁵ following the implementation of the Data Protection Act (Act 843) in 2012 and the formation of the Data Protection Commission of Ghana (DPC) in the same year. Despite these advances, the DPC confronts several operational challenges, including inconsistent enforcement, lack of adequate funding, limited public awareness, and insufficient infrastructure, all of which contribute to a notable gap between policy intentions

³⁹³ Mannion, *supra* note, 350.

³⁹⁴ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

³⁹⁵ African Union, *supra* note 390.

and actual practice.³⁹⁶ Moreover, the DPC's governance structure, which involves appointments by the President and financial oversight by a cabinet minister, raises concerns regarding potential governmental influence, thus questioning the Commission's independence and effectiveness.³⁹⁷

3.7.1 Challenges of Implementing Transplanted GDPR Standards in ECOWAS Member States

The challenges of enforcing data protection standards within the ECOWAS region are not isolated to any single country but are a common issue across several member states, including Benin, Burkina Faso, Mali, Niger, Nigeria, Senegal, and Togo. Despite the establishment of robust legal frameworks, these countries grapple with practical enforcement issues due to various systemic and structural shortcomings.³⁹⁸ In Benin, the Autorité de Protection des Données à caractère Personnel (APDP) faces significant challenges with transparency, particularly regarding the outcomes of its enforcement actions.³⁹⁹ This lack of clarity impacts the authority's perceived effectiveness and undermines its operational credibility. Similarly, Burkina Faso's Commission de l'Informatique et des Libertés (CIL), despite its comprehensive legal mandate, struggles with accountability and public access to information about its activities, which is critical for maintaining public trust in its operations.⁴⁰⁰ Mali has enacted significant legislative reforms to strengthen its data protection regime, starting with Law No. 2013-015⁴⁰¹ and later refined by Law No. 2017-070.⁴⁰² These laws provide a detailed framework for both automated and non-automated data processing, aimed at protecting personal data within Mali's jurisdiction. The designated Data Protection Authority, the APDP, was established to oversee and regulate data protection practices.

³⁹⁶ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

³⁹⁷ *Ibid.*

³⁹⁸ *Ibid.*

³⁹⁹ *Ibid.*

⁴⁰⁰ *Ibid.*

⁴⁰¹ Mali, Law No. 2013-015 of 21 May 2013 on the Protection of Personal Data, data collectors and processors.

⁴⁰² Mali, Law No. 2017-070 Amending Law No. 2013-015 on the protection of personal data.

Despite these measures, the APDP encounters challenges related to the independence of its commissioners and transparency in its enforcement processes.⁴⁰³

Niger's data protection strategy is underpinned by Law No. 2017-28⁴⁰⁴ and its amendment, Law No. 2019-71,⁴⁰⁵ which together create a comprehensive legal environment for the protection of personal data. The *Haute Autorité de Protection des Données à caractère Personnel* (HAPDP) oversees the implementation of these laws. However, it faces issues similar to those in other ECOWAS countries, such as a lack of detailed public reporting on its enforcement activities, which complicates efforts to assess its effectiveness and enforce accountability.⁴⁰⁶ Nigeria's approach to data protection has evolved with the introduction of the NDPR in 2019, implemented by the National Information Technology Development Agency (NITDA) and later overseen by the newly formed Nigeria Data Protection Bureau (NDPB). Despite these developments, the NDPR's implementation faces challenges related to its legal basis and the capacity of regulatory bodies to enforce compliance effectively amidst Nigeria's complex regulatory landscape.⁴⁰⁷

In Senegal, the *Commission des Données Personnelles* (CDP), established under Law No. 2008-12,⁴⁰⁸ is responsible for regulating both automated and non-automated data processing activities. While it has taken proactive steps in issuing fines and processing authorizations, the lack of a public database for penalties and enforcement actions limits transparency and reduces the effectiveness of the regulatory framework.⁴⁰⁹ Togo's legislative framework for data protection, established under Law No. 2019-014,⁴¹⁰ aims to protect privacy and personal freedoms. However, the operationalization of the *Instance de Protection*

⁴⁰³ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴⁰⁴ Niger, Law No. 2017-28 of May 3, 2017, on the Protection of Personal Data Law.

⁴⁰⁵ Niger, Law N° 2019-71 of December 24, 2019 (only available in French), which creates the High Authority for the Protection of Personal Data (HAPDP).

⁴⁰⁶ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴⁰⁷ *Ibid.*

⁴⁰⁸ Senegal, Law No. 2008-12 of January 25, 2008 on the Protection of Personal Data.

⁴⁰⁹ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴¹⁰ Togo, Law No. 2019-014 Relating to the Protection of Personal Data.

des données à caractère Personnels (IPDCP) has been delayed, leaving a significant gap in the enforcement of the law.⁴¹¹ The lack of a functional DPA means that data protection measures are not currently being enforced.

3.7.2 Challenges of Implementing Transplanted GDPR Standards in SADC Member States

The ECOWAS experience is similar to the prevalent issues across the Southern African Development Community (SADC). These countries have also enacted GDPR-inspired laws, facing their own set of obstacles in ensuring effective data protection governance. In Angola, significant strides were made with the enactment of Law 22/11 on Personal Data Protection in 2011, influenced by the EU's Data Protection Directive and Portugal's data protection laws. This comprehensive legislation covers a wide range of data processing activities within the Angolan territory, focusing on principles such as transparency, lawfulness, and proportionality. The *Agência de Proteção de Dados* was established in 2019 to enforce these standards. However, the agency has encountered challenges in developing a robust enforcement mechanism.⁴¹² Despite Angola's legislative framework, the effectiveness of enforcement, particularly in regulating major technology companies, remains insufficiently developed and calls for further enhancement.⁴¹³

Botswana's GDPR-style mandate for an independent DPA (IDPC) stalled for years due to activation delays, revealing bottlenecks in appointments, budgeting, and technical readiness.⁴¹⁴ Though the 2024 Act operationalizes the IDPC, the lag illustrates a broader SADC pattern: laws converge faster than institutions can, creating a persistent implementation gap. Similarly, Lesotho has enacted a Data Protection Act that mandates substantial protections for processing personal data and regulates both domestic and

⁴¹¹ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴¹² *Ibid.*

⁴¹³ *Ibid.*

⁴¹⁴ *Ibid.*

international data handling. The act requires the establishment of a Data Protection Commission (DPC), which has yet to become operational.⁴¹⁵ The absence of this commission severely hampers the enforcement of data protection laws in the country. Appointments to the DPC, controlled by the Prime Minister and subjected to budget approvals by a Minister, have raised concerns about the potential for compromised independence and impartiality, further complicating its operationalization.⁴¹⁶

Madagascar's legal framework under Law No. 2014-038, which comprehensively regulates automated and non-automated processing of personal data, also includes the establishment of the Commission for Informatics and Freedoms (CMIL). However, this body has not yet become operational, leaving a significant enforcement gap and exposing personal data to potential misuse.⁴¹⁷ The CMIL, intended to be managed by a board representing a diverse array of governmental and professional bodies, faces challenges in starting its operations, which undermines the enforcement of data protection regulations.⁴¹⁸ Mauritius represents a more proactive case within the SADC region, aligning its data protection laws closely with European standards to foster foreign investment, particularly in the Information Technology (IT) and Business Process Outsourcing (BPO) sectors.⁴¹⁹ The Data Protection Act of 2017, mirroring GDPR provisions, introduced advanced measures such as mandatory breach notifications and data protection impact assessments.⁴²⁰ While Mauritius has made considerable progress, the practical implementation of these advanced measures continues to evolve,⁴²¹ reflecting the complexities of harmonizing local practices with the GDPR standards. In Seychelles, the Data Protection Act of 2002, designed to protect individuals' privacy rights in relation to personal data processing, has not been activated despite being

⁴¹⁵ *Ibid.*

⁴¹⁶ *Ibid.*

⁴¹⁷ *Ibid.*

⁴¹⁸ *Ibid.*

⁴¹⁹ Alex B. Makulilo, *supra* note 368.

⁴²⁰ *Ibid.*

⁴²¹ *Ibid.*

established over 15 years ago. This lack of enforcement and the absence of a Data Protection Authority, due to the failure to appoint a Commissioner, significantly undermines the protection of personal data. The situation highlights the need for urgent governmental action to establish and activate the Office of the Data Protection Commissioner to align Seychelles with global data protection standards and practices.

South Africa has made considerable advancements with POPIA, which aligns with international data protection standards like the GDPR. Enacted in 2013 and fully implemented in 2020, POPIA was a significant legislative step towards enhancing data privacy. However, the path to compliance has been fraught with challenges, including the nuances of integrating POPIA with the GDPR, which have posed compliance dilemmas for South African entities.⁴²² Lastly, Zambia's recent enactment of the Data Protection Act in 2021 marks a critical step towards establishing a formal data protection framework. The creation of the Office of the Data Protection Commissioner is pivotal for enforcing the act. However, ambiguities regarding the tenure and removal of the Commissioner and the lack of clarity in operational guidelines pose challenges in establishing a robust data protection regime.⁴²³

3.7.3 Challenges of Implementing Transplanted GDPR Standards in East African Countries.

In East Africa, the approach to data protection and privacy rights has seen significant legislative developments in countries like Kenya and Uganda, both of which have established comprehensive legal frameworks modelled after the GDPR. Despite these advances, the region faces ongoing challenges in ensuring effective implementation and enforcement of these regulations. Kenya's Data Protection Act,⁴²⁴ enacted in 2019, aims to regulate both

⁴²² Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴²³ *Ibid.*

⁴²⁴ Kenya, The Data Protection Act, No 24 of 2019.

automated and non-automated processing of personal data involving Kenyan residents, regardless of whether the processing occurs inside or outside the country. This Act led to the establishment of the Office of the Data Protection Commissioner (ODPC), which is charged with a broad range of responsibilities, including overseeing the implementation of the Act, maintaining a register of data controllers and processors, investigating complaints, and imposing administrative penalties.⁴²⁵ Despite its comprehensive mandate, the ODPC struggles with issues of autonomy and effectiveness.⁴²⁶ Concerns about the independence of the ODPC are particularly pronounced given the political influence potential in the appointment and removal processes of the Data Commissioner, who is appointed by the President and confirmed by the National Assembly for a non-renewable six-year term.⁴²⁷ The Commissioner's removal, contingent upon recommendations from the Public Service Commission, introduces a political dimension to what should ideally be an impartial role. Furthermore, the requirement for the Commissioner to submit annual reports to the Cabinet Secretary, who then presents them to the National Assembly, could further impede the ODPC's operational independence.⁴²⁸ Since beginning its operations in November 2020, the ODPC has not disclosed any specific investigations or penalties, which raises concerns about its transparency and the ability to assess its effectiveness in safeguarding data privacy.⁴²⁹

Similarly, Uganda's Data Protection and Privacy Act,⁴³⁰ which officially took effect in May 2019, provides a framework for the regulation of the collection, processing, storage, and use of personal information. This framework applies to any individual, institution, or public body within or outside Uganda that processes personal data relating to Ugandan citizens. The enforcement and oversight of this Act are responsibilities of the Personal Data Protection

⁴²⁵ *Ibid.*

⁴²⁶ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴²⁷ *Ibid.*

⁴²⁸ *Ibid.*

⁴²⁹ *Ibid.*

⁴³⁰ Uganda, The Data Protection and Privacy Act, 2019.

Office (PDPO), which operates under the National Information Technology Authority – Uganda (NITA-U).⁴³¹ The PDPO, led by a director appointed by a Minister of Cabinet for a renewable five-year term, is tasked with overseeing the implementation of the Act, investigating complaints from data subjects, and maintaining a data protection and privacy register.⁴³² One notable enforcement action occurred in January 2021 when the PDPO investigated SafeBoda, a popular ride-hailing app, for unlawfully sharing client data with a U.S.-based data processor.⁴³³ The investigation concluded with recommendations but no fines, reflecting the PDPO's approach to monitoring and enforcing data protection regulations within Uganda.⁴³⁴ The experiences of Kenya and Uganda highlight the broader challenges faced in East Africa regarding data protection legislation and enforcement. While both countries have laid down robust legislative frameworks, issues such as the independence of regulatory bodies, transparency in enforcement actions, and the effective operationalization of these frameworks remain significant hurdles.

Both the Sudan and South Sudan constitutionally recognize the right to privacy. In Sudan, the Constitution enshrines the right to privacy under Section 55, extending this protection to correspondence.⁴³⁵ Despite this constitutional guarantee, Sudan lacks dedicated data protection legislation. Instead, sectoral laws such as the Electronic Transactions Act of 2007, the Cybercrime Act of 2007, and the Cybercrime Prevention (Amendment) Act of 2020 provide limited and fragmented privacy protections.⁴³⁶ These laws address cybercrime and information technology crimes but do not offer a coherent framework for the protection of personal data or establish enforceable rights for individuals regarding their data. Similarly,

⁴³¹ *Ibid.*

⁴³² *Ibid.*

⁴³³ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴³⁴ *Ibid.*

⁴³⁵ Interim National Constitution of the Republic of Sudan, 2005, *art* 55.

⁴³⁶ Sudan: Data Protection Factsheet", *Data Protection Africa* (accessed 1 November 2024), online: <https://dataprotection.africa/sudan/#:~:text=NO%20DATA%20PROTECTION%20LAW>.

South Sudan's Constitution recognizes the right to privacy under Article 22⁴³⁷ and guarantees access to information under Article 32,⁴³⁸ with exceptions to protect individual privacy. However, like Sudan, South Sudan does not yet have a comprehensive data protection framework. Notably, South Sudan is reportedly in the process of drafting a dedicated data protection bill.⁴³⁹ If enacted, this legislation could mark a significant step toward establishing a comprehensive legal framework for personal data protection and addressing the current regulatory vacuum.

3.7.4 Challenges of Implementing Transplanted GDPR Standards in ECCAS Member States

The ECCAS region of Africa, much like its counterparts in ECOWAS and SADC, faces substantial challenges in implementing GDPR-inspired data protection laws effectively. Despite the adoption of comprehensive data protection frameworks, several countries within this region struggle with operational and enforcement issues. Chad's data protection regime, governed by Law No. 007/PR/2015,⁴⁴⁰ sets forth extensive guidelines for the handling of personal data across various entities, whether public or private. The law encompasses a broad spectrum of data processing activities and excludes personal or domestic data not systematically communicated to third parties.⁴⁴¹ The enforcement of this legislation is overseen by the Agence Nationale de Sécurité Informatique et de Certification Électronique (ANSICE), established under Law No. 006/PR/2015.⁴⁴² ANSICE has the authority to issue sanctions and authorizations and is financially autonomous, though it operates under the oversight of the Prime Minister's Office. Despite having a structured governance framework

⁴³⁷ Transitional Constitution of the Republic of South Sudan, 2011, *art* 22.

⁴³⁸ Transitional Constitution of the Republic of South Sudan, 2011, *art* 32.

⁴³⁹ South Sudan: Data Protection Factsheet", *Data Protection Africa* (accessed 1 November 2024), online: <https://dataprotection.africa/south-sudan/#:~:text=DATA%20PROTECTION%20FACTSHEET>.

⁴⁴⁰ Chad, Law No. 007/PR/2015 on the Protection of Personal Data.

⁴⁴¹ *Ibid.*

⁴⁴² Chad, Ordinance No 002/PR/2019 amending Act No 006/PR/2015 on the creation of the National Agency for Computer.

with a Board of Directors appointed by the President, significant transparency and accountability challenges persist, especially notable in its investigation into Facebook in 2020, where details of the outcomes were not publicly disclosed.⁴⁴³ This opacity in enforcement actions undermines public trust and questions the effectiveness of Chad's data protection enforcement framework.⁴⁴⁴

Equatorial Guinea's approach to data protection, defined by Law No. 1/2016,⁴⁴⁵ is aimed at safeguarding individuals' fundamental rights during data processing activities. This law targets registered citizens specifically, raising concerns about its limited scope and the potential exclusion of unregistered individuals.⁴⁴⁶ Crucially, the law calls for the establishment of the Organo Rector de Proteccion de Datos Personales (ORPDP) as the national Data Protection Authority (DPA).⁴⁴⁷ However, the ORPDP has remained non-operational since the law's enactment, with no further regulatory details provided to guide its establishment.⁴⁴⁸ This lack of a functioning DPA creates a significant enforcement gap, leaving personal data at risk and the law largely unenforceable. In Gabon, the data protection framework is detailed in Law No. 001/2011,⁴⁴⁹ which covers both automated and manual data processing activities. The National Commission for the Protection of Personal Data (CNPDCP) is tasked with overseeing these regulations.⁴⁵⁰ Despite its formal independence and the comprehensive scope of its mandate, the CNPDCP struggles with transparency in its operations.⁴⁵¹ Public reports on the CNPDCP's activities, particularly regarding enforcement

⁴⁴³ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴⁴⁴ *Ibid.*

⁴⁴⁵ Equatorial Guinea, Law No 1/2016 on the Protection of Personal Data.

⁴⁴⁶ *Ibid.*

⁴⁴⁷ *Ibid.*

⁴⁴⁸ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴⁴⁹ Gabon, Law No 001/2011 relating to the Protection of Personal Data.

⁴⁵⁰ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴⁵¹ *Ibid.*

actions, are scarce, which complicates the assessment of its effectiveness and hampers accountability.⁴⁵²

The Republic of Congo has also taken legislative steps to bolster data protection with Law No. 29-2019,⁴⁵³ which imposes strict obligations on data controllers and applies to all data processing activities within its jurisdiction. The law stipulates the creation of a Data Protection Authority to ensure adherence to data protection standards.⁴⁵⁴ However, detailed processes for appointing privacy commissioners or establishing the budgetary and operational frameworks for the DPA have not been delineated, resulting in the authority not being officially formed to date.⁴⁵⁵ This absence of a DPA results in significant gaps in enforcement and oversight, greatly hindering the effectiveness of data protection regulations within the country. São Tomé and Príncipe's data protection law, enacted on May 10, 2016,⁴⁵⁶ extends to all data processing activities falling under its jurisdiction and applies to data controllers within and outside the nation, depending on the context of international law.⁴⁵⁷ The National Agency for the Protection of Personal Data (NAPPD), established by this law, functions as an independent administrative entity under the National Assembly. Despite its established structure and significant authority, including the ability to impose fines, the NAPPD faces challenges similar to those in other ECCAS countries, particularly concerning the lack of transparency and public reporting on its operations and decisions.⁴⁵⁸ This deficiency impedes the ability to assess the agency's effectiveness and impacts the overall trust in its enforcement capabilities. Across these countries in the ECCAS region, the recurring themes of inadequate transparency, insufficient accountability, and the non-operational status of designated DPAs

⁴⁵² *Ibid.*

⁴⁵³ Republic of Congo, Law No 29-2019 on the Protection of Personal Data.

⁴⁵⁴ *Ibid.*

⁴⁵⁵ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴⁵⁶ São Tomé and Príncipe, Law No 03/2016 on the Protection of Personal Data.

⁴⁵⁷ *Ibid.*

⁴⁵⁸ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

highlight the broader difficulties faced by countries attempting to align with GDPR-inspired regulations.

3.7.5 Challenges of Implementing Transplanted GDPR Standards in Arab Maghreb Union Member States

In the Arab Maghreb Union, member countries have also undertaken efforts to align with GDPR-inspired data protection standards, yet similar to their counterparts across Africa, they encounter persistent challenges in implementation and enforcement. In Algeria, Law 18-07⁴⁵⁹ was passed in June 2018, designed to regulate both digital and physical processing of personal data, applicable to entities within Algeria and those abroad using processing resources within its borders. Despite the comprehensive nature of the legislation, the implementation has been stalled due to the delay in setting up the necessary Data Protection Authority (DPA), the National Authority for the Protection of Personal Data (NAPP).⁴⁶⁰ The law delineates a broad-based composition for the NAPP, including magistrates, legislative members, human rights councillors, and ministers, which suggests an intent for comprehensive governance in data privacy.⁴⁶¹ However, the failure to establish the DPA has halted the law's enforcement, leaving personal data protections largely theoretical in Algeria.

Similarly, the Republic of Mauritania has laid down a legal framework for data protection with the enactment of Law No. 2017-020⁴⁶² in July 2017. This law aims to regulate the processing of personal data within Mauritania, with exclusions for data used personally or in transit.⁴⁶³ However, the effectiveness of the law is severely compromised by the absence of the crucial implementing decree necessary to bring the law into effect.⁴⁶⁴ Furthermore, the planned Data Protection Authority, the Autorité de Protection des Données à

⁴⁵⁹ Algeria, Law No 18-07 of 25 Ramadhan 1439 (June 10, 2018) relating to the Protection of Individuals in the Processing of Personal Data.

⁴⁶⁰ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴⁶¹ Algeria, Law No 18-07.

⁴⁶² Mauritania, Law No 2017-020 on the Protection of Personal Data.

⁴⁶³ *Ibid.*

⁴⁶⁴ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

caractère personnel (APD), remains non-operational due to the lack of these implementing decrees. The independence and effectiveness of the APD, once established, are also questionable as its operational details and appointment processes remain undefined.⁴⁶⁵ Morocco's approach to data protection is more established, with laws enacted as early as February 18, 2009, covering both automated and non-automated data processing. The National Commission for the Supervision of Personal Data Protection (CNPDP), established by a decree in 2009, is tasked with overseeing data processing activities.⁴⁶⁶ Despite this, the CNPDP's operational independence is potentially compromised as it operates under the Prime Minister's office, with appointments and budgetary allocations influenced by the King and the Prime Minister. While the CNPDP has been proactive in enforcement, issues with transparency persist, notably with delayed and vague reporting that affects public accountability and trust in the data protection regime.⁴⁶⁷

Tunisia stands out as a pioneer in data protection within the region, having integrated personal data protection rights into its Constitution in 2002 and enacting Organic Act No. 2004-63,⁴⁶⁸ which established the Instance nationale de protection des données à caractère personnel (INPDP). While Tunisia made significant legislative advancements, the effectiveness of these measures under an authoritarian regime was limited.⁴⁶⁹ Post-Jasmine Revolution reforms have gradually improved the enforcement mechanisms, though challenges remain, particularly in ensuring the INPDP's independence and its enforcement capabilities.⁴⁷⁰

3.7.6 Enduring Gaps in Implementation

⁴⁶⁵ *Ibid.*

⁴⁶⁶ *Ibid.*

⁴⁶⁷ *Ibid.*

⁴⁶⁸ Tunisia, Organic Act No 2004-63 of July 27, 2004 on the Protection of Personal Data.

⁴⁶⁹ Paradigm Initiative and Olumide Babalola LP, *supra* note 371.

⁴⁷⁰ *Ibid.*

The examples cited from various regions across Africa highlight a shared theme: while legislative frameworks often align with international standards, the actual enforcement and operational transparency required to make these laws effective are frequently lacking. The efforts to harmonize privacy and data protection legislation across Africa face significant and varied challenges. These challenges highlight the complexity of implementing a standardized legal framework like the GDPR in regions with diverse legal, cultural, and socio-economic backgrounds. While some African countries have made notable progress in aligning their data protection laws with global standards, systemic and structural issues, such as insufficient autonomy of privacy and data protection agencies, inconsistent enforcement, and lack of adequate resources, persistently undermine these efforts. These obstacles are further complicated by the direct importation of European legal standards without sufficient adaptation to local realities.

3.8 Conclusion

The GDPR marks a significant evolution in the EU's approach to privacy and data protection, establishing a rigorous standard that has repercussions far beyond its borders. While the GDPR is lauded for its comprehensive protection of privacy rights within the EU, its stringent requirements present notable challenges for non-EU countries, particularly those in Africa. The application of the GDPR model in African countries reveals significant limitations and challenges. Its prescriptive and often inflexible requirements do not easily align with the diverse legal, economic, and cultural contexts found across African nations. The imposition of the GDPR's framework onto African countries can inadvertently suppress local innovation and impose burdensome regulatory obligations that are not suited to the technological or economic realities of these nations. Moreover, the EU's approach, with its heavy emphasis on compliance and the potential for severe penalties, does not necessarily translate into effective data protection in environments with different legal traditions and

enforcement capabilities. The GDPR's focus on individual rights and privacy, while commendable, often clashes with communal or collective values that are prevalent in many African societies, leading to a disconnect between the regulation and its practical implementation. In particular, African societies emphasize collective well-being and interdependence, which contrasts with the GDPR's individualistic emphasis on personal autonomy and control over data. This cultural divergence requires a more nuanced and adaptable regulatory approach that respects communal values while still safeguarding personal privacy.

The challenges of adopting the GDPR in Africa highlight the need for a more flexible and contextually appropriate approach to data protection. This would involve developing regulations that not only protect personal data but also respect and reflect local values and needs, fostering regulations that enhance rather than hinder the growth of the digital economy. In conclusion, while the GDPR sets a valuable benchmark for privacy and data protection, its wholesale adoption poses significant challenges for African countries. These nations must navigate a complex balance between meeting international data protection standards and fostering a regulatory environment that supports innovation and economic growth within their unique contexts. To achieve this balance, it is critical to ensure that privacy laws in Africa reflect communal norms and cultural priorities, allowing for harmonization between global standards and local practices. A nuanced approach, taking into consideration the specific needs and conditions of each country, is essential for creating effective data protection frameworks in Africa.

Chapter 4: Evaluating African Union and Regional Organizations' Efforts in Data Protection and Privacy.

4.1 Introduction

The EU's GDPR has emerged as a foundational framework for global data protection laws, establishing a benchmark that has been widely adopted and promoted across various jurisdictions, including Africa.⁴⁷¹ Since the enactment of the GDPR, this influence has only intensified, with the GDPR positioning itself as a model that many countries look to when developing their data protection regimes. Scholars such as Patricia Boshe, Moritz Hennemann, and Ricarda von Meding refer to this phenomenon as a *race to the GDPR*,⁴⁷² as the EU actively exports its standards globally. This trend has found considerable traction in Africa, where numerous countries have developed data protection laws that align closely with the GDPR model.⁴⁷³ As of today, 36 African countries have enacted comprehensive data protection laws that embody principles consistent with EU standards, demonstrating the GDPR's influence on both national and regional regulatory frameworks.

This chapter addresses the mechanisms, frameworks, and initiatives that exist within Africa to regulate privacy and data protection, critically evaluating their effectiveness and limitations in the face of Africa's evolving digital landscape. In doing so, it examines how closely these frameworks align with the GDPR's model while questioning the adequacy of a Eurocentric approach in addressing the specific needs and values of African societies. While GDPR principles provide a robust foundation, the African context presents distinct challenges

⁴⁷¹ Scott, Mark, and Laurens Cerulus. "Europe's new data protection rules export privacy standards worldwide." *Politico*, January 31, 2018, 12:00 PM CET. Accessed April 17, 2024. <https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/>.

⁴⁷² Patricia Boshe, Moritz Hennemann & Ricarda von Meding, "African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward," *Global Privacy Law Review* 3, no. 2 (2022): 56-64.

⁴⁷³ A.B. Makulilo, *African Data Privacy Laws*, Law, Governance and Technology Series, vol. 33 (Springer International Publishing AG, 2016) at 198.

and priorities, particularly due to the continent's unique socio-cultural, economic, and political context. Data protection efforts in Africa have been largely responsive to the global digital revolution and the exponential rise in data processing. As digital transformation accelerates across African economies, the need for secure and adaptive data protection frameworks becomes critical.⁴⁷⁴ However, merely transposing European standards may overlook the nuances of Africa's socio-cultural dynamics, where privacy and data governance are embedded within community-centric values rather than individualistic approaches. Therefore, the AU and its RECs face the dual challenge of upholding international standards while ensuring these frameworks resonate with African social realities.

In the regulatory frameworks of the EU and the AU, distinct approaches to privacy and data protection reflect differing regional priorities. The EU framework, grounded in Article 8 of the Charter of Fundamental Rights of the European Union,⁴⁷⁵ emphasizes data protection as a fundamental human right. This legal architecture is marked by principles that prioritize individual autonomy, transparency, and strict controls on cross-border data transfers. In contrast, the AU's approach is situated within a broader agenda of digital governance, which includes not only data privacy but also cybersecurity, cybercrime, and the promotion of digital innovation.⁴⁷⁶ This inclusive approach is seen in the AU Convention on Cybersecurity and Personal Data Protection (the Malabo Convention), which integrates data protection within the broader issues of digital transformation.⁴⁷⁷ Adopted in 2014 and entered into force in 2023 upon the 15th ratification, the Malabo Convention exemplifies the AU's commitment to a unified approach that addresses Africa's diverse and interconnected digital challenges.⁴⁷⁸ While the GDPR-inspired frameworks highlight Africa's integration into global data

⁴⁷⁴ Bitange Ndemo, Njuguna Ndung'u, Scholastica Odhiambo, and Abebe Shimeles, eds., *Data Governance and Policy in Africa* (Springer International Publishing, 2023), <https://doi.org/10.1007/978-3-031-24498-8> Accessed April 17, 2024.

⁴⁷⁵ *Charter of Fundamental Rights of the European Union*, 2000 O.J. (C 364) 1.

⁴⁷⁶ *Preamble, African Union Convention on Cyber Security and Personal Data Protection*, African Union, 2014.

⁴⁷⁷ *Ibid.*

⁴⁷⁸ *Ibid.*

protection standards, the AU's framework acknowledges the need for a flexible and context-sensitive approach to privacy.⁴⁷⁹ The Malabo Convention, for instance, incorporates provisions on digital governance that are specifically tailored to address Africa's digitalization goals, including economic integration and secure cross-border data flows.⁴⁸⁰ However, one major limitation of the Malabo Convention is its slow adoption rate, which reflects varying levels of readiness and capacity among member states. Countries like Angola, Egypt, and Senegal have ratified the Convention, yet its uptake across the continent remains uneven, accentuating the challenges of implementing a uniform data protection regime across diverse legal and political environments.⁴⁸¹ The Economic Community of West African States (ECOWAS) has played a pivotal role in regional data protection, especially through its Supplementary Act A/SA.1/01/10, which has set binding standards across West Africa. This Act demonstrates an approach akin to treaty frameworks, creating a binding legal instrument that fosters alignment among member states without superseding national sovereignty.

Beyond the GDPR's influence, African RECs such as COMESA and SADC have embraced varied strategies to facilitate data protection governance that respects the continent's unique characteristics. This nuanced regulatory environment recognizes that African countries cannot rely solely on binding EU-inspired regulations; rather, they require adaptable legal instruments that reflect local priorities and capacities. As such, COMESA employs binding regulations to ensure uniformity, while SADC favours model laws that allow member states the flexibility to adapt data protection principles to suit national

⁴⁷⁹ *Ibid.*

⁴⁸⁰ African Union, *Digital Transformation Strategy for Africa 2020–2030*, Addis Ababa, May 18 2020, at pp 8–11

⁴⁸¹ DataGuidance, "Africa: Malabo Convention - A Pan-African Strategy for Data Protection," online: DataGuidance <https://www.dataguidance.com/opinion/africa-malabo-convention-pan-african-strategy-data>, accessed October 30, 2024.

contexts.⁴⁸² This adaptive approach is essential in a region where soft laws and cooperative agreements play a critical role in reconciling diverse cultural and legal traditions. However, the reliance on non-binding frameworks presents inherent challenges, particularly in achieving consistent enforcement and effective oversight.

In light of these complexities, the AU has developed initiatives such as the Digital Single Market (DSM) strategy⁴⁸³ and the Data Policy Framework,⁴⁸⁴ which aim to establish harmonized legal standards that balance innovation with privacy protection. These initiatives are aligned with the AfCFTA⁴⁸⁵ and emphasize the importance of data sovereignty, digital rights, and economic integration. Importantly, the AU's frameworks encourage African states to engage as active participants in global data policy dialogues, advocating for a digital ecosystem that reflects Africa's values and aspirations rather than passively adopting external standards.⁴⁸⁶ By advocating for principles such as collective privacy rights and data stewardship, the AU seeks to create a governance model that supports Africa's socio-cultural priorities.

This chapter is structured into four comprehensive parts, each focusing on different aspects of data protection and privacy within the African context. The first part examines the constitutional foundations of privacy and data protection across African countries, exploring the early support for these rights through constitutional provisions inspired by international norms like the UDHR and ICCPR. Additionally, this section discusses the varied approaches among African countries, from explicitly incorporating personal data protection into

⁴⁸² Alex B. Makulilo, "One Size Fits All: Does Europe Impose Its Data Protection Regime on Africa?," *Datenschutz und Datensicherheit* 37, no. 447 (2013): 450; Graham Greenleaf & Bertil Cottier, "Comparing African Data Privacy Laws: International, African and Regional Commitments," *University of New South Wales Law Research Series* 26 (2020); Lukman Abdulrauf, "Giving 'Teeth' to the AU Towards Advancing Compliance with Data Privacy Norms," *Information & Communications Technology Law* 30, no. 87 (2021): 88 et seq.

⁴⁸³ Graham Greenleaf & Bertil Cottier, "International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis," *Computer Law & Security Review* 44 (2022): 105638, <https://doi.org/10.1016/j.clsr.2021.105638> Accessed on April, 2024.

⁴⁸⁴ *African Union Data Policy Framework*, endorsed by the AU Executive Council, February 2022.

⁴⁸⁵ *Africa Continental Free Trade Agreement (AfCFTA)*, adopted 21 March 2018, entered into force 30 May 2019.

⁴⁸⁶ *African Union, Data Policy Framework, Feb. 2022, at pp 57-60.*

constitutions to recognizing privacy as a fundamental human right. It also assesses the impact of European standards, particularly the GDPR, on these frameworks and the inconsistent application of these influences across different nations.

The second part focuses on the AU's role, particularly through the Malabo Convention, and examines the AU Data Policy Framework, detailing its objectives, challenges, and successes. The third part addresses efforts to harmonize data protection laws across Africa through initiatives by RECs such as ECOWAS, SADC, ECCAS, CEMAC, and EAC, and explores contributions from entities like the Association of Francophone Data Protection Authorities. This section emphasizes the challenges in achieving uniform data protection standards, noting variations in scope and enforcement across the continent.

Finally, the fourth part provides a comprehensive analysis of REC-led harmonization efforts, focusing on how these communities align data protection standards influenced by historical and legal traditions. It also considers the impact of European frameworks, such as EU directives and Council of Europe conventions, and highlights the complexities of legal harmonization due to different levels of adoption and adaptation across regions. The chapter emphasizes the broader continental effort toward standardizing data protection regulations, illustrated through ECOWAS's success in establishing a more coherent regime, and highlights the remaining challenges in achieving a unified framework across Africa. This analysis not only highlights the substantial role played by the AU in advancing data protection but also reinforces the necessity for an approach that aligns more closely with African realities. By examining these frameworks critically, this chapter lays the groundwork for further discussions on how Africa can advance a privacy and data protection regime that genuinely reflects its cultural, social, and legal uniqueness.

4.2 Constitutional Foundations and Developments in Privacy and Data Protection Across Africa

Before 2001, privacy and data protection in African countries were predominantly upheld through constitutional rights.⁴⁸⁷ These constitutions, formed during the independence movements of the 1960s and 1970s, incorporated liberal and human rights principles reflecting international norms like those in the Universal Declaration of Human Rights (UDHR)⁴⁸⁸ and the International Covenant on Civil and Political Rights (ICCPR).⁴⁸⁹ Article 12 of the UDHR emphatically states:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

This is mirrored in Article 17 of the ICCPR which specifies:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. And 2. Everyone has the right to the protection of the law against such interference or attacks.

These constitutional rights broadly shield against arbitrary searches, restrict undue collection and processing of personal data regarding family and private matters, and preserve the privacy of communications.⁴⁹⁰ As a result, individuals are empowered to uphold their rights and pursue remedies for violations through legal or human rights avenues.⁴⁹¹

⁴⁸⁷ Patricia Boshe, Moritz Hennemann & Ricarda von Meding, *supra* note 472.

⁴⁸⁸ *Universal Declaration of Human Rights* (UDHR), adopted by the General Assembly on 10 December 1948, GA Res 217A (III), UN Doc A/810 at 71 (1948).

⁴⁸⁹ *International Covenant on Civil and Political Rights* (ICCPR), adopted 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

⁴⁹⁰ See Art. 46, *Constitution of Algeria* (1996) "The protection of individuals when handling personal data shall be a fundamental right guaranteed by law ..."; Arts. 32-34, *Constitution of Angola* (2010); Arts. 20-21, *Constitution of Benin* (1990); Art. 9, *Constitution of Botswana* (1966); Art. 28, *Constitution of Burundi* (2018); Art. 6, *Constitution of Burkina Faso* (1991); Art. 27, *Constitution of Comoros* (2018); Art. 49, *Constitution of Chad* (2018); Art. 26, *Constitution of the Republic of Congo* (2015); Art. 31, *Constitution of the Democratic Republic of Congo* (2005); Arts. 12-13, *Constitution of Djibouti* (1992); Arts. 57-58, *Constitution of Egypt* (2014); Art. 26, *Constitution of Ethiopia* (1994); Art. 1(5), *Constitution of Gabon* (1991); Art. 23, *Constitution of Gambia* (1997); Art. 42, *Draft Constitution of Gambia* (2019); Art. 12, *Constitution of Guinea* (2010); Arts. 44, 48, *Constitution of Guinea-Bissau* (1984); Art. 31, *Constitution of Kenya* (2010); Art. 22, *Constitution of the Kingdom of Swaziland* (2005); Arts. 10-11, *Constitution of Lesotho* (1993); Arts. 11-13, *Libya Transitional Constitution* (2011); Art. 35, *Draft Constitution of Libya* (2017); Art. 13, *Constitution of Madagascar* (2010);

Although the African Charter on Human and Peoples' Rights⁴⁹² does not explicitly mention the right to privacy, it implies this right through the protections afforded to life and human dignity. Article 4 of the Charter states, "*Human beings are inviolable. Every human being shall be entitled to respect for his life and the integrity of his person.*" This indicates that an individual's dignity is compromised when their privacy is unlawfully infringed. Furthermore, the African Commission on Human and Peoples' Rights in its 'Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa' (2015),⁴⁹³ identifies privacy as an inferred right, recognizing the integral role of human dignity in its protection. Against this historical backdrop, the contemporary landscape of constitutional recognition and legal frameworks for privacy and data protection across Africa shows significant diversity.

In African countries, the constitutional acknowledgment of privacy and data protection varies widely. As of 2024, only seven African countries, Algeria, Angola, Cape Verde, Gabon, Mozambique, Seychelles, and Tunisia, explicitly incorporate personal data

Art. 21, *Constitution of Malawi* (1994); Art. 6, *Constitution of Mali* (1992); Art. 9, *Constitution of Mauritius* (1968); Art. 24, *Constitution of Morocco* (2011); Art. 13, *Constitution of Namibia* (1990); Art. 29, *Constitution of Niger* (2010); Art. 37, *Constitution of Nigeria* (1999); Arts. 21, 23, *Constitution of Rwanda* (2003); Art. 14, *Constitution of South Africa* (1996); Art. 19, *Somali Provisional Constitution* (2012); Art. 13, *Constitution of Senegal* (2001); Art. 22, *South Sudan Transitional Constitution* (2011); Art. 55, *Constitution of Sudan* (2019); Art. 37, *Constitution of Sudan* (2005); Art. 29, *Constitution of Sudan* (1973); Art. 16, *Constitution of Tanzania* (1977); Art. 28, *Constitution of Togo* (1992); Art. 24, *Constitution of Tunisia* (2014); Art. 27, *Constitution of Uganda* (1995); Arts. 11(d), 17, *Constitution of Zambia*; Art. 15, *People's Republic of Zanzibar Constitution* (1984); Art. 57, *Constitution of Zimbabwe* (2013).

⁴⁹¹ Arts. 18, 105, *Constitution of Botswana* (court); Art. 114, *Constitution of Benin* (court); Art. 60, *Constitution of Burundi* (court); Art. 125, *Constitution of Burkina Faso* (court); Arts. 5, 37, *Constitution of Gambia* (court); Arts. 5, 33, 34, 183(b), *Draft Constitution of Gambia* (2019); Art. 33, *Constitution of Kenya* (court); Arts. 146, 32, *Constitution of Guinea* (Conacry) (court and National Institution of Human Rights); Art. 32, *Constitution of Guinea-Bissau* (court); Art. 164, *Constitution of the Kingdom of Swaziland*; Arts. 15(1), 129, *Constitution of Malawi* (court and Human Rights Commission); Art. 17, *Constitution of Mauritius* (court); Arts. 24(2), (3), (4), *Constitution of Namibia* (court); Art. 44, *Constitution of Niger* (Human Rights Commission); Art. 46, *Constitution of Nigeria* (court); Art. 67, *Constitution of Sudan* (court and Human Rights Commission); Art. 9(4), *Constitution of South Sudan* (court and Human Rights Commission); Arts. 38–39, *Constitution of South Africa* (court); Arts. 125, 129, *Constitution of Tanzania* (court and Human Rights Commission); Arts. 99, 104, *Constitution of Togo* (court); Art. 128, *Constitution of Tunisia* (Human Rights Commission); Arts. 50, 51, 58, *Constitution of Uganda* (court and Human Rights Commission); Arts. 28, 230, *Constitution of Zambia* (court and Human Rights Commission); Art. 215, *Constitution of the Republic of Congo* (court). Also see, Graham Greenleaf & Bertil Cottier, *supra* note 4.

⁴⁹² *African Charter on Human and Peoples' Rights*, adopted 27 June 1981, OAU Doc CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982) (entered into force 21 October 1986).

⁴⁹³ African Commission on Human and Peoples' Rights, *Principles and Guidelines on Human and Peoples' Rights while Countering Terrorism in Africa*, Part 11 (2015).

protection into their constitutions.⁴⁹⁴ Conversely, 28⁴⁹⁵ of the 55 African countries constitutionally recognize privacy as a fundamental human right, with specific articles dedicated to this right. Additionally, twelve countries explicitly safeguard the secrecy of communications.⁴⁹⁶ However, seven countries⁴⁹⁷ do not explicitly mention privacy rights in their constitutions. The effectiveness of these constitutional protections varies, resulting in uneven enforcement and legal recourse.

The lack of extensive case law on constitutional protections of privacy, as noted by Alex Makulilo,⁴⁹⁸ suggests that this is an area still in need of further legal development and clarification. Differences in approach to data protection provisions can also be seen among the countries that have specific constitutional references to data protection. For example, Algeria,⁴⁹⁹ Angola,⁵⁰⁰ and Gabon⁵⁰¹ have tasked their legislatures with developing data protection laws but have not detailed the requirements of these laws. In contrast, Seychelles⁵⁰² and Mozambique⁵⁰³ have gone further by not only mandating legislation but

⁴⁹⁴ Art. 47, *Constitution of Algeria*; Arts. 32-34, *Constitution of Angola* (2010); Art. 45, *Constitution of Cape Verde*; Art. 1(5), *Constitution of Gabon* (1991); Art. 71, *Constitution of Mozambique*; Art. 10, *Constitution of Seychelles*; Art. 24, *Constitution of Tunisia* (2014).

⁴⁹⁵ *Constitution of Burkina Faso*, art. 6; *Constitution of Burundi*, art. 23; *Constitution of the Republic of Chad*, art. 17; *Constitution of the Democratic Republic of the Congo*, art. 31; *Constitution of the Arab Republic of Egypt*, art. 57; *Constitution of the State of Eritrea*, art. 18; *Constitution of the Federal Democratic Republic of Ethiopia*, art. 26; *Constitution of the Republic of Guinea*, art. 12; *Constitution of Guinea Bissau*, art. 44; *Constitution of the Republic of Kenya*, art. 31; *Constitution of the Kingdom of Lesotho*, art. 4; *Constitution of the Republic of Liberia*, art. 16; *Constitution of Libya*, art. 12; *Constitution of the Republic of Malawi*, art. 21; *Constitution of the Republic of Mali*, art. 6; *Constitution of the Islamic Republic of Mauritania*, art. 13; *Constitution of the Kingdom of Morocco*, art. 24; *Constitution of the Republic of Namibia*, art. 13; *Constitution of the Federal Republic of Nigeria*, art. 37; *Constitution of Rwanda*, art. 23; *Constitution of the Democratic Republic of Sao Tome and Principe*, art. 23; *Constitution of the Republic of Sierra Leone*, art. 15; *Constitution of the Republic of South Africa*, art. 14; *Constitution of the Republic of South Sudan*, art. 22; *Constitution of Sudan*, art. 37; *Constitution of the United Republic of Tanzania*, art. 16; *Constitution of the Republic of Uganda*, art. 27; *Constitution of Zimbabwe*, art. 57.

⁴⁹⁶ *Constitution of the Republic of Benin*, art. 21; *Constitution of the Republic of Cameroon*, Preamble; *Constitution of the Central African Republic*, art. 18; *Constitution of the Republic of the Congo*, art. 26; *Constitution of the Republic of Djibouti*, art. 13; *Constitution of the Republic of Equatorial Guinea*, art. 1; *Constitution of the Republic of The Gambia*, art. 23; *Constitution of the Republic of Ghana*, art. 18; *Constitution of the Republic of Madagascar*, art. 13; *Constitution of the Republic of Niger*, art. 29; *Constitution of the Republic of Senegal*, art. 13; *Constitution of the Togolese Republic*, art. 29.

⁴⁹⁷ Botswana (only privacy of the home), Comoros, Ivory Coast, Mauritius, Somalia, Swaziland and Zambia.

⁴⁹⁸ Makulilo, Alex B. "African Data Privacy Laws" (2016) Law, Governance and Technology Series.

⁴⁹⁹ *Constitution of the People's Democratic Republic of Algeria*, Article 46, revised 2020.

⁵⁰⁰ *Constitution of the Republic of Angola*, Article 32, adopted in 2010.

⁵⁰¹ *Constitution of the Gabonese Republic*, Article 1.6, revised in 2018.

⁵⁰² *Constitution of the Republic of Seychelles*, Article 28, revised in 1993.

also embedding essential principles of data protection, such as access rights and purpose limitation, directly into their constitutions. Tunisia's Constitution⁵⁰⁴ uniquely safeguards personal data alongside privacy and telecommunications secrecy. Cape Verde⁵⁰⁵ stands out for its detailed constitutional provisions that comprehensively cover data protection aspects, ensuring robust frameworks for privacy and data security.

Despite the variations in constitutional provisions, the regime of privacy and data protection in African countries demonstrates notable diversity and complexity. The absence of specific constitutional provisions on personal data protection or privacy rights does not necessarily impede the development of robust data protection legislation. For instance, Ivory Coast and Mauritius, which do not explicitly recognize privacy rights in their constitutions, have nonetheless implemented some of the most advanced data protection laws in Africa.⁵⁰⁶ Conversely, Mozambique, despite having strong constitutional safeguards for data privacy, has yet to establish comprehensive data protection legislation. Moreover, evaluating the overall legal framework for privacy in any jurisdiction requires a review that extends beyond sector-specific statutes, a consideration that exceeds the scope of this thesis. The ensuing analysis sets the stage for understanding how privacy and data protection are integrated within the broader context of human rights frameworks in Africa.

4.2.1 African Human Rights Frameworks: Data Protection and Privacy Considerations

The concept of privacy in African countries has traditionally been viewed through the lens of human rights but privacy has not been universally recognized as a fundamental right

⁵⁰³ *Constitution of the Republic of Mozambique*, Article 71, adopted in 2004.

⁵⁰⁴ *Constitution of the Republic of Tunisia*, Article 24, adopted in 2014.

⁵⁰⁵ *Constitution of the Republic of Cape Verde*, Articles 45 and 46, revised in 2010.

⁵⁰⁶ Ivory Coast and Mauritius have established comprehensive data protection frameworks. Ivory Coast's Law No. 2013-450, enacted on June 19, 2013, regulates personal data handling, focusing on individual rights and sensitive data processing requirements. Mauritius's Data Protection Act of 2017, aligns closely with the GDPR, detailing the responsibilities of data controllers and establishing the Data Protection Office as the regulatory authority.

specifically addressing data protection, unlike in Europe where both privacy and data protection are explicitly addressed. In Africa, discussions generally focus on data privacy without emphasizing data protection, although some legal frameworks integrate these concepts, suggesting that protecting privacy inherently includes data protection.⁵⁰⁷ A closer look at the African Charter on Human and Peoples' Rights⁵⁰⁸ and the African Charter on the Rights and Welfare of the Child⁵⁰⁹ reveals how these foundational instruments address privacy implicitly, despite not explicitly recognizing it as a separate right. The African Charter on Human and Peoples' Rights, known as the Banjul Charter, was established in 1981 to set foundational standards for human rights protection across Africa. While all African countries, except South Sudan, have ratified this Charter, it notably does not specifically mention the right to privacy or private life. However, it contains provisions that implicitly uphold privacy rights, such as the inviolability of the human person,⁵¹⁰ rights to life and personal integrity,⁵¹¹ entitlements to liberty and security.⁵¹² Regarding the privacy rights of minors, the African Charter on the Rights and Welfare of the Child, effective from 1990, addresses privacy concerns, highlighting Africa's commitment to safeguarding privacy among children.⁵¹³

Additionally, these implicit privacy protections are further reinforced through the mechanisms established to ensure compliance and resolve disputes. To enforce these rights, the African Commission on Human and Peoples' Rights monitors compliance through periodic reviews and handles complaints, although its direct influence on privacy issues is

⁵⁰⁷ For example, *Data Protection and Privacy Act, 2019* (Act No. 9 of 2019), Uganda. This legislation was enacted to regulate the processing of personal data and to protect the privacy of individuals.

⁵⁰⁸ *African Charter on Human and Peoples' Rights*, adopted 27 June 1981, OAU Doc CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982) (entered into force 21 October 1986).

⁵⁰⁹ *African Charter on the Rights and Welfare of the Child*, adopted 11 July 1990, OAU Doc. CAB/LEG/24.9/49 (1990), entered into force 29 November 1999.

⁵¹⁰ *African Charter on Human and Peoples' Rights* (ACHPR), *supra* note 508, article 4.

⁵¹¹ *Ibid*, article 5.

⁵¹² *Ibid*, article 6.

⁵¹³ *African Charter on the Rights and Welfare of the Child*, *supra* note 509, article 10.

limited due to the Charter's broad language.⁵¹⁴ The Commission has emphasized the need for robust privacy safeguards within broader human rights protections.⁵¹⁵ Additionally, the African Human Rights Court (AHRC), established in 2006, provides a judicial mechanism for dispute resolution,⁵¹⁶ though its authority is directly recognized by only a few states such as Benin, Burkina Faso, and Côte d'Ivoire. Notably, some states have withdrawn their authorizations allowing direct NGO or individual appeals, reflecting the complex and evolving legal landscape of privacy protections in Africa, intertwined with the broader spectrum of human rights.⁵¹⁷ This framework of human rights and privacy protections provides a foundational context for understanding the varying degrees of privacy and data protection legislation across the continent.

4.2.2 An overview of African Countries with privacy and data protection legislation

A critical analysis of the data protection framework in Africa highlights significant disparities in the adoption, maturity, and enforcement of privacy and data protection laws across the continent. These variations reflect the broader influence of external frameworks, such as the EU's GDPR,⁵¹⁸ and reveal the diverse legal, economic, and political contexts within which these laws operate. Several African countries, including South Africa, Kenya, Ghana, Nigeria, Rwanda, and Uganda, have developed comprehensive privacy and data protection frameworks. These legal systems often mirror the GDPR, incorporating stringent standards on data handling and enforcement mechanisms.⁵¹⁹ This category also includes

⁵¹⁴ *Resolution on the Right to Freedom of Information and Expression on the Internet in Africa*, ACHPR/Res. 362(LIX) 2016; *The General Comments on Article 14(1)(d) and (e) of the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa*, which interprets Article 14's mandate for self-protection to include the right to privacy.

⁵¹⁵ *Ibid.*

⁵¹⁶ *The 1999 Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights*, particularly article 34 (6).

⁵¹⁷ Graham Greenleaf & Bertil Cottier, *supra* note 134.

⁵¹⁸ *Ibid.*

⁵¹⁹ *Ibid.*

nations such as Morocco, Tunisia, Senegal, Mali, Niger, Togo, Burkina Faso, Cote d'Ivoire, Chad, Gabon, Angola, Eswatini, and Sao Tome and Principe.⁵²⁰ The adoption of such frameworks demonstrates a proactive stance toward data protection, with clear enforcement measures in place. However, these efforts raise questions about the adaptability of externally influenced frameworks to the local socio-economic realities of these nations. In contrast, countries such as Egypt, Madagascar, Seychelles, Cameroon, Lesotho, Gambia, Equatorial Guinea, Burundi, and Congo have limited data protection frameworks. While progress has been made, their legal instruments often lack comprehensive coverage or suffer from inconsistent enforcement.⁵²¹ This partial adoption highlights the challenges these countries face in aligning their frameworks with global data protection standards, particularly when regulatory capacity and resources are constrained. More critically, several African countries, including Namibia, Libya, Mozambique, Sudan, Guinea Bissau, Mauritania, Malawi, Liberia, South Sudan, Guinea, Western Sahara, Ethiopia, Eritrea, Somalia, Djibouti, Central African Republic, and the Democratic Republic of Congo, operate without formal privacy or data protection laws.⁵²² This regulatory gap could hinder these countries from participating fully in the global digital economy, perpetuating economic dependencies. Beyond the GDPR, the AU and RECs play a critical role in this scenario, facilitating the adaptation and enforcement of privacy and data protection laws tailored to the continent's unique needs.⁵²³ Their efforts focus on promoting regional data protection standards that respect the diverse cultural and legal nuances of each member state. Through cooperative initiatives, they aim to address the challenges depicted on the map, advocating for the widespread adoption and effective enforcement of comprehensive data protection laws across Africa.

⁵²⁰ *Ibid.*

⁵²¹ Patricia Boshe, Moritz Hennemann & Ricarda von Meding, *supra* note 472.

⁵²² Graham Greenleaf & Bertil Cottier, *supra* note 134.

⁵²³ *Ibid.*

As African countries strive to overcome disparities in data protection, significant legislative efforts are evident across the continent. Currently, thirty-six (36) out of fifty-five (55) African countries have established data protection laws or regulations, highlighting a commitment to enhancing legal and regulatory frameworks.⁵²⁴ The AU Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention, exemplifies these efforts. Adopted on June 27, 2014, and officially effective from June 8, 2023, following its ratification by fifteen countries, the Convention highlights the regional dedication to cyber security and data protection.⁵²⁵ Notably, Eswatini has introduced its first data protection legislation, the Data Protection Act of 2022, effective from March 4, 2022.⁵²⁶ This act governs both local and foreign data controllers and processors operating within Eswatini, utilizing automated or non-automated means to process personal data.⁵²⁷ The law reflects the influence of EU standards, incorporating core GDPR principles such as purpose limitation⁵²⁸ and data minimization,⁵²⁹ and introducing similar legal bases for data processing. In Tanzania, the enactment of the Personal Data Protection Act 2022⁵³⁰ represents a broader update, including revisions to the Electronic Transactions Act and the Electronic and Postal Communications Act,⁵³¹ reflecting a holistic approach to managing data protection and privacy in the digital age.

Recognizing the complexities of data protection, African countries are integrating cybercrime and cybersecurity laws into their data protection strategies, as demonstrated by

⁵²⁴ Data Protection Africa, a special project developed by ALT Advisory, provides comprehensive information on data protection laws, access to data protection authorities, and trends in African countries. The platform features Fact Sheets for each country, entries on case law, legislative trends, and directories of organizations involved in data protection, available in 18 languages. Available at: <https://dataprotection.africa/> accessed on June 11, 2024. ALT Advisory is a public interest advisory group based in South Africa, focusing on emerging human rights issues in Africa and globally.

⁵²⁵ *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention), *supra* note 378.

⁵²⁶ ALT Advisory, *supra* note 524.

⁵²⁷ *Ibid.*

⁵²⁸ *Data Protection Act, 2022* (Act No. 5 of 2022), s 12 (Eswatini).

⁵²⁹ *Ibid.*, section 13.

⁵³⁰ DataGuidance, "Tanzania Data Protection Overview" (only available in Kiswahili), available at <https://www.dataguidance.com/notes/tanzania-data-protection-overview>, accessed on June 11, 2024.

⁵³¹ *Ibid.*

the AU Malabo Convention.⁵³² This approach acknowledges the multifaceted nature of data protection in the digital age and provides a comprehensive legal framework to address these issues. Enhancements in regulatory structures and enforcement mechanisms are evident across the continent. For instance, Uganda's passage of the Computer Misuse (Amendment) Act 2022 strengthens data protection measures, particularly concerning children's data.⁵³³ In Algeria, the National Authority for the Protection of Personal Data has become operational following the initial legislation passed in 2018.⁵³⁴ Botswana has improved international data transfer protocols, recognizing both EU member states and African countries like Kenya and South Africa as jurisdictions with adequate data protection standards.⁵³⁵ These legislative and regulatory improvements reflect a growing recognition of the importance of privacy and data protection. While these efforts are heavily influenced by GDPR standards, African countries are taking a broader approach by considering cybercrime and cybersecurity aspects, creating a distinct framework.

4.2.3 European Influence and International Commitments in African Privacy and Data Protection Legislation

The influence of EU frameworks, particularly the GDPR, on African data protection laws is both significant and complex. European standards have not only shaped global benchmarks for privacy but have also heavily influenced the development of national legislative frameworks across Africa. This influence is largely driven by a range of international obligations and regional agreements that African states are party to, such as the AU's initiatives and broader international conventions like the ICCPR. For instance, all African

⁵³² *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention), *supra* note 378.

⁵³³ Preamble, *Computer Misuse (Amendment) Act, 2022*, (Uganda).

⁵³⁴ ALT Advisory, *supra* note 524.

⁵³⁵ *Botswana, Data Protection Act, 2024 (Act 18 of 2024), Part VIII (ss 50–54)*.

countries except Comoros and South Sudan have ratified the ICCPR,⁵³⁶ which upholds the right to privacy in Article 17. Further demonstrating global engagement, African countries actively participate in the Council of Europe's Data Protection Convention 108⁵³⁷ and its modernization, Convention 108+,⁵³⁸ which align with standards similar to the EU's 1995 Data Protection Directive and the more recent GDPR, albeit in a more generalized format. Despite being nicknamed GDPR Lite,⁵³⁹ the modernized Convention has seen active adoption and implementation by African countries, reflecting the significant EU influence in shaping data protection standards across Africa.

The reach of this influence is further exemplified through the EU's adequacy assessments, which determine whether a non-EU country's data protection regime meets EU standards, a prerequisite for allowing the unhindered transfer of personal data from the EU to that country.⁵⁴⁰ Although no African country has yet received a positive adequacy decision, Mauritius has actively sought to meet these standards by modifying its laws to align with EU prerequisites.⁵⁴¹ This highlights the significant impact of EU policies on African data privacy legislation, as the EU's stringent standards, exemplified by the GDPR, continue to set the benchmark for data protection worldwide. This influence is evident not only in the adoption of similar standards in conventions like Convention 108+ but also in the ongoing efforts by African countries to align their laws with the GDPR to facilitate international trade and data

⁵³⁶ *International Covenant on Civil and Political Rights* (ICCPR), adopted 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

⁵³⁷ *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108), Council of Europe, opened for signature 28 January 1981, ETS No. 108 (entered into force 1 October 1985).

⁵³⁸ *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108+), Council of Europe, opened for signature 10 October 2018, CETS No. 223 (entered into force on the date of its ratification by the member states).

⁵³⁹ Graham Greenleaf, "Modernised' Data Protection Convention 108 and the GDPR," *Privacy Laws & Business International Report*, no. 154 (2018): 22-23, [2019] UNSWLRS 3, <https://ssrn.com/abstract=3279984> Accessed on April 18, 2024.

⁵⁴⁰ *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* (General Data Protection Regulation), [2016] OJ L 119/1, art 45.

⁵⁴¹ DLA Piper Africa, "New Hurdles to Transferring European Personal Data to Mauritius," available at <https://www.dlapiperafrica.com/en/mauritius/insights/2021/new-hurdles-to-transferring-european-personal-data-to-mauritius.html>, accessed on June 11, 2024.

exchanges. While African countries engage with multiple international data privacy frameworks, the pervasive influence of European legal standards, especially the GDPR, highlights the complexities they face in balancing regional commitments with global data protection norms.

However, this strong European influence raises critical concerns about the suitability of these frameworks within the African socio-cultural and legal context. The GDPR, with its emphasis on individual rights and stringent compliance requirements, is grounded in a distinctly European legal and philosophical tradition that prioritizes personal autonomy and market-based protections. This contrasts sharply with many African societies, where privacy is often understood in communal, relational terms rather than as an individual right. For example, in rural African communities, decisions about the sharing and use of personal data are often made collectively, with elders or community leaders playing a pivotal role.⁵⁴² The GDPR's focus on individual consent overlooks these collective decision-making processes, potentially alienating local communities from the very protections the law seeks to provide. The imposition of European standards such as the GDPR not only disregards the communal nature of African societies but also risks erasing local traditions that emphasize collective over individual responsibility.

Moreover, the strict regulatory demands of the GDPR, such as the requirement for Data Protection Officers, the complex rules governing data transfers, and the mandate for breach notifications within 72 hours, are often unfeasible in many African countries, which lack the necessary technological infrastructure and institutional capacity. These stringent requirements place a disproportionate burden on African states, diverting scarce resources from developing more contextually appropriate privacy protections. The wholesale transplantation of these

⁵⁴² Mutua, Jacqueline N., and Timothy Mwangi Kiruhi. "Village Elders' Participation in Public Governance in Kenya: A Phenomenological Study." *Open Journal of Leadership*, vol 10, no 2, 2021, pp. 110-128. <https://www.scirp.org/journal/paperinformation?paperid=109778>, accessed October 31, 2024.

frameworks fails to account for the diversity of Africa's legal environments, its varied levels of technological development, and its different economic priorities. This reflects a broader issue of imposing foreign legal standards that are misaligned with the socio-economic realities of the Global South.

While these European frameworks are regarded as global gold standards, their imposition on African countries can be viewed as a continuation of colonial legal practices, where foreign norms and standards are prioritized over homegrown solutions. By focusing primarily on aligning with European frameworks, African countries miss a critical opportunity to develop data protection laws that reflect their unique socio-cultural, legal, and economic contexts. This dynamic perpetuates a form of legal dependency, where African states are seen as passive recipients of European norms rather than as active participants in shaping global data governance. The reliance on these European models also raises concerns about the lack of agency African states have in defining their regulatory systems, with these standards often enforced to meet external demands, such as trade agreements or international partnerships, rather than internal needs.

4.3 The Malabo Convention: A Comprehensive Legal Framework for Cyber Security and Data Protection in Africa

The AU Convention on Cyber Security and Personal Data Protection marks a significant milestone in the legal and strategic framework for information security across Africa. However, while it presents itself as a landmark framework, the Convention's ability to fully reflect the diverse socio-cultural and economic realities of the African continent remains questionable. The Convention was adopted with the foresight of consolidating existing regional and international commitments, the Convention aims to foster a vibrant Information

Society on the continent.⁵⁴³ Rooted in the Constitutive Act of the African Union of 2000,⁵⁴⁴ the Convention reflects a collective resolve among African states to enhance their legislative environment concerning Information and Communication Technologies (ICTs).⁵⁴⁵ However, a deeper critique reveals that the Convention's alignment with existing global frameworks, especially those rooted in European standards, raises concerns about its ability to create a truly African-oriented data protection regime. The Convention explicitly aims to solidify the objectives of Africa's Information Society but also to fortify the underlying legal frameworks that govern ICT operations across the member states and the RECs.⁵⁴⁶ This pivotal legal document reaffirms the Member States' commitment to uphold fundamental human and peoples' rights, referencing key declarations and conventions both within the AU and under the United Nations.⁵⁴⁷ Despite its clear commitment to human rights and privacy, the Convention does not appear to fully integrate the collective, communal understanding of privacy that is deeply embedded in many African societies. Instead, its reliance on international standards such as those found in the EU's GDPR raises questions about whether it sufficiently accommodates African socio-cultural contexts.

In addition to its focus on privacy, the Convention establishes a comprehensive framework for cybersecurity, recognizing the need for adaptive security measures that can foster a trusted digital environment, facilitate electronic transactions, and combat cybercrime.⁵⁴⁸ It also sets out the procedural and substantive legal foundations necessary for combating cybercrime, calling for the modernization of criminal laws to introduce specific

⁵⁴³ *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention), *supra* note 378.

⁵⁴⁴ *Constitutive Act of the African Union*, adopted 11 July 2000, entered into force 26 May 2001.

⁵⁴⁵ *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention), *supra* note 378.

⁵⁴⁶ *Ibid.*

⁵⁴⁷ *Ibid.*

⁵⁴⁸ *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention), *arts.* 8-15, *supra* note 378.

ICT-related offences.⁵⁴⁹ However, while this modernizing agenda is crucial, it again reflects a legal transference of external models rather than the development of solutions uniquely tailored to African realities. African states, with their varied technological infrastructures and legal traditions, may struggle to fully implement the prescribed security frameworks, which mirror those in more developed regions.

The Malabo Convention's dual emphasis on both cybersecurity and personal data protection offers a broad approach to managing privacy and data protection challenges across Africa. It reflects a strategy that ostensibly accommodates the diverse legal, cultural, and economic realities of African countries. However, the extent to which this framework addresses the unique socio-cultural dynamics of Africa is debatable. For example, while the Convention proposes a balanced framework that respects citizens' rights to privacy while promoting the free flow of information, it fails to incorporate African communal privacy structures into its legal provisions. This omission reflects a broader issue within many African privacy laws, which are often heavily modelled on external, particularly European, legal standards, rather than being adapted to fit the continent's socio-legal contexts. The Convention has been lauded as Africa's first significant regional instrument for data protection, often compared to the Council of Europe's Convention 108.⁵⁵⁰ As of June 8, 2023, the Malabo Convention secured the necessary 15 ratifications to come into force, indicating its growing acceptance and implementation.⁵⁵¹ Yet, its comparison to European frameworks like Convention 108 further highlights the extent to which African data protection laws continue to be influenced by external legal standards. While the Malabo Convention is a critical step forward, its design and implementation reflect the challenges African states face in balancing international legal obligations with local needs and customs.

⁵⁴⁹ *Ibid.*

⁵⁵⁰ Hlomani, Hanani, and Caroline B. Ncube. "Data Regulation in Africa: Free Flow of Data, Open Data Regimes and Cybersecurity." In *Data Governance and Policy in Africa*, edited by Bitange Ndemo, Njuguna Ndung'u, Scholastica Odhiambo, and Abebe Shimeles, 97-130. Cham, Switzerland: Palgrave Macmillan, 2023.

⁵⁵¹ *Ibid.*

The Malabo Convention's influence is particularly notable among countries like Namibia, Mozambique, and Rwanda, which operate under a monist legal system where ratified international treaties immediately become part of national law.⁵⁵² This seamless integration of international frameworks into domestic legal systems illustrates the continued dominance of external legal models in African legislative processes. Rather than fostering a distinctly African approach to data protection and cybersecurity, the Convention risks reinforcing the same legal dependency that has characterized much of Africa's legal evolution in the post-colonial era. While it offers a structured framework for legal reform, it does not adequately engage with the potential for creating more contextually relevant privacy and data protection frameworks that reflect African communal and customary laws.

4.3.1 Data Protection Framework of the Malabo Convention

The Malabo Convention, while representing a significant development for data protection in Africa, is heavily shaped by European data protection standards. It defines personal data broadly, much like the European frameworks, with a definition that encompasses any information that could directly or indirectly identify an individual.⁵⁵³ Similarly, the Convention outlines the role of data controllers and establishes clear guidelines on how data is processed, both manually and through automated means.⁵⁵⁴ Article 9 extends the Convention's scope to cover both the public and private sectors, though it introduces exemptions for processing related to public security, defence, state security, and scientific research, provided these activities are legally justified.⁵⁵⁵ However, the influence of European

⁵⁵² See Namibia, *Constitution of the Republic of Namibia*, 1990, art 144; Mozambique, *Constitution of the Republic of Mozambique*, 2004 (rev 2007), art 18(1)–(2); Rwanda, *Constitution of the Republic of Rwanda*, 2003 (rev 2015), art 168.

⁵⁵³ African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), *article 1*, *supra* note 378.

⁵⁵⁴ *Ibid.*

⁵⁵⁵ *Ibid.*, Article 14.

standards raises concerns about whether these exemptions and the framework as a whole, adequately reflect Africa's unique socio-cultural contexts.

One significant distinction in the Malabo Convention's approach is its inclusion of parental filiation as sensitive personal data,⁵⁵⁶ which is a recognition of the deeply rooted cultural significance of lineage and familial ties in many African societies. This represents a notable effort to adapt to Africa's socio-cultural realities, where such information may carry legal and social implications, particularly in matters of inheritance or social standing. Yet, despite these culturally relevant provisions, the Convention remains largely influenced by European standards, particularly the GDPR, which does not account for such regional nuances. The Malabo Convention's selective adaptation highlights the challenge of creating a truly contextually tailored framework, where European models dominate, but some regional adjustments are made. The Convention does attempt to diverge from European frameworks in its approach to cross-border data transfers. Unlike the GDPR, which mandates an adequate level of protection for transfers between European states, the Malabo Convention focuses on data transfers outside the African Union.⁵⁵⁷ This suggests an attempt to prioritize regional autonomy within Africa, allowing member states greater flexibility in managing intra-African data flows. However, for transfers outside the AU, the Convention still mandates that data controllers ensure adequate protections, subject to approval from national Data Protection Authorities (DPAs).⁵⁵⁸ While this may reflect a nuanced response to Africa's socio-political diversity, it also highlights the continued influence of international, particularly European, standards in shaping African legal frameworks.

Moreover, the Malabo Convention mirrors several core GDPR principles, such as the requirement for transparency in data processing and the mandate for explicit consent in

⁵⁵⁶ Art. 10(5)(d), *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention). See also Graham Greenleaf & Bertil Cottier, *supra* note 4 at 134.

⁵⁵⁷ Art. 12 (K), *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention).

⁵⁵⁸ *Ibid*, article 14 (6) (a).

processing sensitive personal data.⁵⁵⁹ However, it does not adopt some of the more stringent GDPR measures, such as specific rules governing direct marketing or immediate breach notifications.⁵⁶⁰ This flexibility could be seen as an attempt to accommodate the diverse governance needs of African states, but it also raises questions about whether the framework is robust enough to handle the complexities of Africa's rapidly evolving digital environment. The Convention's omission of direct marketing regulations, for instance, reflects a deliberate choice to allow flexibility in areas that may not align with the current digital and regulatory capacities of many African states. While this flexibility may serve Africa's short-term needs, it also risks creating gaps in protection that could become problematic as Africa's digital environments continue to develop.

Despite its attempts to address Africa's unique data protection needs, the Malabo Convention remains largely constrained by the influence of European models. Its reliance on Western legal frameworks, while adapted in some areas, raises critical questions about whether the Convention sufficiently acknowledges the collective, community-centric nature of African privacy norms. The challenge lies in determining whether the Malabo Convention effectively reconciles these tensions, or whether it replicates European models without fully contextualizing them for African realities. While the Convention offers rights similar to those found in the GDPR, such as the right to access,⁵⁶¹ rectify,⁵⁶² or oppose the processing of personal data,⁵⁶³ it remains rooted in principles of individual privacy. This emphasis on individual rights, rather than collective or communal rights, highlights the underlying tension between Western legal concepts and African socio-cultural values. The absence of detailed

⁵⁵⁹ Art. 13, Principle 1, *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention).

⁵⁶⁰ This restriction is provided in Chapter 1 of the *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention) on the framework for electronic transactions. See Art. 6, Malabo Convention.

⁵⁶¹ African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), *article 17*, *supra* note 378.

⁵⁶² *Ibid*, article 19.

⁵⁶³ *Ibid*, article 18.

regulations on direct marketing and cross-border data flows, along with the flexible framework for data transfers, indicates that the African Union sought to balance regional flexibility with international alignment. However, this balance may come at the cost of neglecting key elements of Africa's communal privacy norms, which often stand in tension with the more individualistic privacy protections found in the GDPR. While the Convention represents a step toward harmonizing data protection across Africa, its provisions reflect a continuing dependency on external models that may not fully address Africa's diverse socio-cultural contexts.

4.3.2 Influence of the Convention on National Legal Frameworks

The AU Convention on Cybersecurity and Personal Data Protection, which came into effect on June 8, 2023, has undeniably influenced data protection legislation across member states. However, despite its significance, the Convention largely reflects a methodology aligned with European data protection standards, raising questions about its ability to foster truly homegrown legal frameworks in Africa. While the Convention offers a comprehensive model for data protection, its heavy reliance on external standards limits the capacity of member states to develop uniquely African approaches that reflect their specific legal, cultural, and economic contexts. The Convention serves as a model act, providing member states with a comprehensive framework that they can adopt directly or modify to fit their national contexts.⁵⁶⁴ This approach, while facilitating the uniform adoption of data protection practices, risks perpetuating the top-down imposition of external legal models, rather than encouraging African states to innovate and create frameworks that are better suited to their local realities. The administrative demands of implementing the Convention are considerable, particularly for countries with limited resources and institutional capacity. While the Convention supports the establishment of strong data governance frameworks, it does so

⁵⁶⁴ Preamble, *African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention).

through a lens heavily influenced by European standards, which may not always align with Africa's diverse legal systems and communal privacy values.

One of the Convention's strengths is its alignment with other regional data protection efforts, such as the ECOWAS Supplementary Act⁵⁶⁵ and the SADC Data Protection Model Law.⁵⁶⁶ This coherence is essential for harmonizing data protection laws across the continent. However, the harmonization process itself presents challenges, as it often involves the transplantation of foreign legal norms into African contexts without adequate consideration of whether these norms are suitable for Africa's socio-cultural and legal environments. While consistency in data protection laws is valuable, the focus on regional and international alignment can overshadow the need for laws that resonate with the local practices and values of African societies. Since its adoption in 2014 during the 23rd Ordinary Session of the Assembly in Malabo, the Convention has attracted varied levels of engagement among the 55 AU member states. As of September 19, 2023, 19 countries have signed the Convention, and 15 have ratified and deposited it, legally binding themselves to its terms.⁵⁶⁷ The ratification process highlights the gradual pace of implementation, which reflects both the complexities of aligning national laws with international standards and the broader challenge of ensuring that these laws are contextually appropriate for each country. For some countries, the adoption of the Convention represents a significant step forward in enhancing their cybersecurity and data protection standards. However, the heavy reliance on a European-style framework may inhibit the development of more context-sensitive legal solutions that are attuned to Africa's communal and collective privacy norms.

⁵⁶⁵ *Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS*, adopted 16 February 2010, Economic Community of West African States.

⁵⁶⁶ *SADC Model Law on Data Protection*, Southern African Development Community, adopted 2013.

⁵⁶⁷ *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection* (Malabo Convention), updated as of 19 September 2023. Available at:

[https://au.int/sites/default/files/treaties/29560-sl-AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION0.pdf](https://au.int/sites/default/files/treaties/29560-sl-<u>AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION</u><u>0.pdf</u>), accessed on June 12, 2024.

Notable among the ratifying states are Angola and Ghana, both of which have emerging digital economies and are regional leaders in technology adoption.⁵⁶⁸ Angola ratified the Convention in 2020,⁵⁶⁹ and Ghana in 2019,⁵⁷⁰ marking important milestones in their commitment to advancing digital security measures. Yet, the question remains whether these advancements are driven by a genuine effort to create regionally tailored frameworks or are part of a broader strategy to align with international standards that prioritize external, particularly European, trade and regulatory partnerships. Other countries, including Cape Verde, Côte d'Ivoire, Congo, Guinea, Mauritania, Mauritius, Mozambique, Namibia, Niger, Rwanda, Senegal, Togo, and Zambia, have also ratified and deposited the Convention, signalling a regional commitment to implementing a harmonized data protection framework.⁵⁷¹ However, even with this regional push, the extent to which these frameworks reflect Africa's diverse legal traditions and socio-cultural dynamics remains debatable.

Despite the gradual adoption rate, the Convention plays a crucial role in shaping the future of data protection and cybersecurity across Africa. Yet, this influence may come at a cost if it continues to reinforce a dependency on external legal frameworks rather than encouraging the development of authentically African solutions. The Convention's reliance on a model that closely mirrors European standards raises important questions about the capacity of African states to assert their legal sovereignty and develop frameworks that are not only harmonized across the continent but also deeply rooted in Africa's unique legal and cultural contexts.

4.3.3 Strategic Advancements in Digital Governance: The African Union's Data Policy Framework

⁵⁶⁸ *Ibid.*

⁵⁶⁹ *Ibid.*

⁵⁷⁰ *Ibid.*

⁵⁷¹ *Ibid.*

In a parallel effort to strengthen digital governance across the continent, the AU's Data Policy Framework, adopted in February 2022, marks a significant step forward in Africa's digital strategy. However, while this framework is a key component of a broader initiative aimed at enhancing data governance, its alignment with established international data protection standards raises concerns about whether it fosters truly African-centric solutions or further embeds external legal and regulatory models. Designed to envision a unified digital space that secures and allows for the free flow of data, the framework seeks to empower African countries to capitalize on the opportunities of a data-driven economy.⁵⁷² Yet, the extent to which it succeeds in integrating Africa's unique socio-cultural and economic contexts remains a critical point of analysis. Further expounded on July 28, 2022, the Framework emerged from extensive multi-stakeholder consultations and is intended to serve as a comprehensive, multi-year guide for the AU's efforts to develop a robust digital economy.⁵⁷³ While it clearly defines strategic priorities to establish a cohesive data framework, the strategic alignment with international regulatory frameworks, particularly from Western economies, prompts questions about whether Africa is charting its course in data governance or following in the footsteps of global powers. The vision of a DSM is undoubtedly a forward-looking initiative, but its success hinges on how well African countries can align this framework with their specific legal, technological, and social realities.

Building on the foundational principles of the AU Convention on Cybersecurity and Personal Data Protection, the Framework seeks to refine and expand these principles by fostering cross-sectoral collaborations essential for developing data infrastructure and regulatory mechanisms.⁵⁷⁴ However, this strategic approach, while laudable for its ambition,

⁵⁷² African Union, *AU Data Policy Framework*, February 2022. Available at <https://www.au.int/en/documents/20220518/au-data-policy-framework>, accessed on June 11, 2024.

⁵⁷³ *Ibid.*

⁵⁷⁴ *Ibid.*

may not fully account for the significant disparities in infrastructure capabilities, governance frameworks, and socio-political contexts across African countries. The attempt to align data governance laws across member states could streamline data management, but it also risks overshadowing the specific local needs and values of individual countries, many of which are still grappling with fundamental infrastructure challenges. The question remains whether harmonizing data protection laws across the continent will come at the cost of neglecting the diverse legal traditions and socio-cultural imperatives that define Africa's governance structures.

The Data Policy Framework did not emerge in isolation but builds on previous initiatives such as the Digital Transformation Strategy of 2020,⁵⁷⁵ the AfCFTA,⁵⁷⁶ and the Policy and Regulatory Initiative for Digital Africa.⁵⁷⁷ These efforts laid the groundwork to address the unique opportunities and challenges presented by the digital economy. However, while the framework highlights the dual nature of data as both a valuable asset and a potential risk, its regulatory approach seems primarily influenced by established international norms, raising concerns about how these global standards are reconciled with Africa's socio-legal realities. For instance, the framework supports data sovereignty but opposes excessive data localization requirements that might infringe on human rights,⁵⁷⁸ advocating instead for selective localization to facilitate cross-border data flows.⁵⁷⁹ This selective approach may reflect the influence of global data governance debates, but the deeper question is whether

⁵⁷⁵ *AU Data Policy Framework*, presented at the Sixth Meeting of the Intergovernmental Group of Experts on E-commerce and the Digital Economy, Geneva, 10-12 May 2023. This framework was endorsed by the African Union Executive Council, detailing strategic initiatives to harness data for socio-economic development, enhance interoperability of systems, and facilitate cross-border data flows to realize a single African digital market. Available at https://unctad.org/system/files/non-official-document/ige6_ecde_p04_Amazouz_en.pdf Accessed on May 10, 2024.

⁵⁷⁶ *Africa Continental Free Trade Agreement* (AfCFTA), adopted 21 March 2018, entered into force 30 May 2019.

⁵⁷⁷ *Policy and Regulatory Initiative for Digital Africa* (PRIDA), launched by the African Union, the European Union, and the International Telecommunication Union, initiated in 2018.

⁵⁷⁸ African Union, *AU Data Policy Framework*, February 2022. Available at <https://www.au.int/en/documents/20220518/au-data-policy-framework>, accessed on June 11, 2024.

⁵⁷⁹ *Ibid.*

Africa is setting its priorities or responding to pressures from international trade and regulatory regimes.

Furthermore, the Framework promotes innovative practices suitable for the African context, such as reinforcing collective privacy rights and encouraging the development of data stewardships or trusts.⁵⁸⁰ Yet, translating these principles into practical implementation faces significant challenges, particularly given the uneven stages of technological and regulatory development among member states.⁵⁸¹ The disparity in infrastructure and governance capacities complicates efforts to harmonize and uniformly adopt these policies across the continent. Without significant investment in infrastructure and capacity-building, there is a risk that these ambitious goals may remain largely aspirational, failing to address the real disparities in digital governance capabilities across Africa.

Despite these challenges, the Data Policy Framework and the Convention have achieved notable milestones, highlighting a growing political commitment across the continent to utilize data as a catalyst for regional development.⁵⁸² Nevertheless, the question of whether these initiatives will ultimately position Africa as a leader in global digital policy or simply as a standard adopter remains critical. The Framework has undoubtedly improved cooperation among AU member states, regional economic communities, and the private sector, but its dependence on alignment with international norms could limit Africa's ability to assert its sovereignty in digital governance. While the Framework aims to harmonize regional data governance and improve cross-border data flows, the deeper issue is whether this harmonization process genuinely reflects African realities or if it is an externally driven initiative, mirroring the global regulatory frameworks of Western economies. The successes of these initiatives have laid the groundwork for a more integrated and harmonized digital governance framework across Africa, positioning the continent to establish an African

⁵⁸⁰ *Ibid.*

⁵⁸¹ *Ibid.*

⁵⁸² *Ibid.*

DSM.⁵⁸³ However, the ongoing success of these policies will depend on sustained commitment, financial support, and technical collaboration among member states. As Africa works to build a more unified digital economy, it must balance the need for alignment with international standards with the imperative of developing frameworks that reflect its governance priorities, socio-cultural values, and economic needs. Without this balance, the risk remains that Africa will continue to serve as a follower in global digital policy rather than emerging as a proactive standard-setter.

4.4 Privacy and Data Protection Instruments of African Regional Economic Communities (RECs)

Across Africa, there is a growing effort to align data protection laws within various sub-regions, facilitated by the continent's RECs. These RECs, including the Economic Community of West African States (ECOWAS),⁵⁸⁴ the Southern African Development Community (SADC),⁵⁸⁵ the Economic Community of Central African States (ECCAS),⁵⁸⁶ the Central African Economic and Monetary Community (CEMAC),⁵⁸⁷ and the East African Community (EAC),⁵⁸⁸ play an integral role in the regional harmonization of privacy and data protection policies. However, this alignment is significantly shaped by historical ties and linguistic affiliations, which often dictate the adoption of legal frameworks heavily influenced by European standards. In regions where French, English, or Portuguese prevail, the accessibility of national laws and international data protection instruments in these languages enhances their integration into local legislation.⁵⁸⁹ Yet, this linguistic integration

⁵⁸³ *Ibid.*

⁵⁸⁴ *Economic Community of West African States* (ECOWAS), established by the Treaty of Lagos, 28 May 1975.

⁵⁸⁵ *Southern African Development Community* (SADC), established by the Treaty of Windhoek, 17 August 1992.

⁵⁸⁶ *Economic Community of Central African States* (ECCAS), established by the Treaty of Libreville, 18 October 1983.

⁵⁸⁷ *Central African Economic and Monetary Community* (CEMAC), established by the Treaty of N'Djamena, 16 March 1994.

⁵⁸⁸ *East African Community* (EAC), established by the Treaty for the Establishment of the East African Community, signed on 30 November 1999, entered into force on 7 July 2000.

⁵⁸⁹ Graham Greenleaf & Bertil Cottier, *supra* note 134.

reflects a deeper concern about the extent to which Africa's privacy laws are shaped by external legal norms rather than being developed to reflect the continent's unique socio-cultural dynamics.

Many African countries model their data protection laws on European frameworks, particularly the EU's legal instruments and the Council of Europe's conventions, available in French and English.⁵⁹⁰ The Association of Francophone Data Protection Authorities (AFAPDP), for example, plays a significant role in French-speaking African countries by facilitating dialogue, enhancing capacity building, and promoting consistency in data protection standards.⁵⁹¹ While this initiative has been successful in fostering cross-border cooperation among Francophone states, the reliance on EU models raises concerns about whether these frameworks are adaptable to Africa's distinct legal traditions and communal privacy values. This dynamic represents a complex mosaic of national priorities, regional harmonization efforts, and international influences that filter through linguistic and cultural channels. The challenge is whether these influences leave enough room for African countries to assert legal sovereignty in data governance.

Despite these structured regional initiatives, broader efforts to align these frameworks at the continental level, spearheaded by the AU and the RECs, face significant challenges in creating a cohesive data protection environment across Africa. The varying scope and level of protection offered by the AU's and RECs' frameworks point to a lack of coherence and uniformity, preventing the establishment of a standardized approach to data protection regulation across the continent.⁵⁹² This lack of harmonization is compounded by the frameworks' reliance on the 1995 DPD, a model that, although modernized through the

⁵⁹⁰ *Ibid.*

⁵⁹¹ *Ibid.*

⁵⁹² For a detailed comparison between African data protection laws and the abovementioned instruments, *ibid.*, at 26.

GDPR, is rooted in European regulatory traditions.⁵⁹³ This continued reliance on European-derived standards raises critical questions about their effectiveness and appropriateness for addressing the needs of Africa's digital economy and regulatory environment.⁵⁹⁴ The reliance on an external standard that does not fully reflect Africa's socio-cultural and technological context suggests a potential mismatch between the legal frameworks in place and the continent's unique challenges and opportunities.

However, despite these challenges, some RECs have made significant strides in fostering more harmonized data protection regimes. For instance, the ECOWAS has demonstrated considerable progress in developing a more coherent data protection framework across its member states. This progress highlights the potential for African regional organizations to drive the development of privacy and data protection laws that reflect local needs. Yet, the broader challenge remains: whether these regional successes can be scaled up to the continental level without being overshadowed by the pervasive influence of external, particularly European, legal models.

4.4.1 Regional Integration and Data Protection Initiatives in The Economic Community of West African States (ECOWAS)

The ECOWAS, which encompasses fifteen diverse countries where French, Portuguese, and English are the principal languages, has been at the forefront of data protection advancements in West Africa.⁵⁹⁵ However, while ECOWAS has made significant strides in establishing a regional legal framework for data protection, the extent to which these efforts are shaped by external influences, particularly from the EU, raises critical questions about the sovereignty and adaptability of these laws within the African context. The

⁵⁹³ Patricia Boshe, Moritz Hennemann & Ricarda von Meding, *supra* note 472; and Graham Greenleaf & Bertil Cottier, *supra* note 134.

⁵⁹⁴ *Ibid.*

⁵⁹⁵ *Economic Community of West African States* (ECOWAS) comprises fifteen member countries: Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, and Togo, established by the Treaty of Lagos, 28 May 1975

Revised Treaty of ECOWAS, ratified by member states in 2008, laid the groundwork for the enactment of data privacy laws across the community. This commitment was actualized through the Supplementary Act on Personal Data Protection within ECOWAS in 2010, which not only mandates the establishment of data protection laws in each member state but also delineates the structural requirements for data protection authorities.⁵⁹⁶ While this represents a significant regional achievement, it is important to examine whether the legal frameworks developed through this act are truly reflective of West Africa's socio-cultural realities or if they primarily mirror external legal models.

The Supplementary Act is a binding regional data protection agreement in effect across West Africa, with its provisions enforceable by the ECOWAS Court of Justice, thereby reinforcing its authority.⁵⁹⁷ However, the influence of European models on the development of ECOWAS's legal frameworks is evident. The act's development was facilitated by collaborative efforts between the EU and the ITU from 2005 to 2007, initiatives that would later evolve into the Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA).⁵⁹⁸ This collaboration highlights the significant role external actors play in shaping Africa's data governance landscape. While such international partnerships can bring valuable expertise, they also risk overshadowing the development of homegrown legal frameworks that are better suited to African contexts. In 2011, ECOWAS further enhanced its data protection framework with Directive C. Dir. 1/08/11, which addresses cybercrime within the region and criminalizes violations of the established principles and formalities for processing personal data as detailed in the Supplementary Act.⁵⁹⁹ This comprehensive legal framework is aimed at

⁵⁹⁶ *Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS*, adopted 16 February 2010, Economic Community of West African States.

⁵⁹⁷ *ECOWAS Court of Justice*, established under the Protocol A/P.1/7/91 on the Community Court of Justice, Economic Community of West African States.

⁵⁹⁸ *Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA)*, an initiative supported by the International Telecommunication Union (ITU) and the European Commission, aimed at improving ICT policy frameworks in the region.

⁵⁹⁹ *Directive C/DIR. 1/08/11 on Fighting Cybercrime within ECOWAS*, issued August 2011, aims to adapt substantive criminal law and procedures in ECOWAS member states to address cybercrime, including various

ensuring robust protection of personal data across the ECOWAS region. Yet, the extent to which this framework reflects a distinctly African approach to data protection remains a subject of critical analysis. The heavy involvement of external actors in the drafting and implementation of these policies raises concerns about the influence of European norms on what should ideally be a legal framework tailored to the socio-cultural and economic realities of West Africa.

The comprehensive regional approach laid out by ECOWAS set the stage for the subsequent alignment seen in the AU Convention on Cybersecurity and Personal Data Protection, which closely mirrors the principles and structure established by the ECOWAS Act. While this alignment is indicative of a broader pan-African effort to standardize data protection regulations, it also prompts further questions about the dominance of external legal models, particularly European ones, in shaping these frameworks. The risk, therefore, is that the process of harmonization and standardization, while promoting regional integration, may inadvertently entrench Africa's reliance on external legal models, leaving limited room for the development of truly African data protection regimes.

4.4.2 Regional Adaptations in Data Protection: Comparing the AU Malabo Convention and ECOWAS Supplementary Act

The AU Convention on Cyber Security and Personal Data Protection draws significant influence from the earlier ECOWAS Supplementary Act on Personal Data Protection, reflecting a notable alignment between the two legal frameworks. However, while both frameworks aim to establish effective data protection regimes across Africa, it is essential to critically examine whether these legal instruments genuinely reflect African socio-cultural realities or if they replicate external, particularly European legal models. The connection between the two documents is clear, as they share many similarities in terms of

types of cybercrimes, sanctions, and procedural rules. Available at: <https://dig.watch/resource/directive-fighting-cybercrime-within-ecowas> Accessed on June 11, 2024.

scope and the underlying principles governing data protection. Yet, this alignment raises important questions about whether Africa's regional bodies are creating frameworks that reflect local needs or if they are primarily influenced by global standards.

Both the Malabo Convention and the ECOWAS Supplementary Act mandate specific data processing formalities, such as requiring notifications⁶⁰⁰ and obtaining authorization from respective Data Protection Authorities.⁶⁰¹ They also emphasize the establishment of independent national DPAs to ensure oversight and adherence to data protection norms.⁶⁰² While these are critical steps toward strengthening data protection across the continent, it is important to recognize that these formalities, though necessary, are largely modeled on international data protection regimes, particularly the European Union's GDPR. This raises concerns about whether these frameworks adequately reflect African governance structures, where the role of oversight and accountability may be viewed differently due to unique socio-cultural and political contexts. Despite the many similarities between the Malabo Convention and the ECOWAS Supplementary Act, there are also notable differences that reflect some degree of regional adaptation. For instance, the AU Convention emphasizes the principle of proportionality, requiring that processed data be adequate, relevant, and not excessive.⁶⁰³ This principle of data minimization, which is less emphasized in the ECOWAS framework, suggests a deliberate effort by the AU to introduce more stringent controls on data processing, reflecting evolving global concerns about data privacy. However, the adoption of such principles still raises the question of whether this approach is tailored to Africa's specific needs or whether it mirrors global trends, particularly those emanating from Europe.

⁶⁰⁰ ECOWAS, "ECOWAS Data Protection Act," Article 9; African Union, "African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)," *Article* 10.

⁶⁰¹ ECOWAS, "ECOWAS Data Protection Act," Chapter 3; African Union, "African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)," *Article* 12.

⁶⁰² *Ibid.*

⁶⁰³ African Union, "African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)," *Art. 13, princ. 3(b)*.

Moreover, the AU Convention's emphasis on data minimization and proportionality introduces a more nuanced approach to privacy regulation compared to the ECOWAS framework. This distinction illustrates that while regional frameworks may share foundational principles, their implementation and focus areas can diverge, reflecting both regional priorities and external influences. However, even with these distinctions, both frameworks still face the challenge of ensuring that their provisions are not merely transplanted from external models but are adapted to Africa's own socio-political and legal environments. The similarities between these frameworks highlight a broader trend of alignment within African data protection laws. Yet, this trend also highlights the continued influence of external legal models, particularly the EU's GDPR, on African data protection frameworks. While the harmonization of regional and continental legal instruments can facilitate the creation of more consistent and predictable data protection regimes across Africa, it also risks entrenching a dependency on external norms, rather than fostering the development of truly African privacy and data protection frameworks that are responsive to the continent's unique challenges.

4.4.3 Data Protection Laws Enacted within the ECOWAS Region

Within the ECOWAS, twelve out of fifteen member states have enacted their own data protection laws, reflecting a growing commitment to privacy and data security across the region. However, the establishment of these laws raises critical questions about the extent to which they reflect African legal autonomy or whether they are primarily shaped by external European models, particularly the French approach to data protection. Before the adoption of the ECOWAS Supplementary Act in 2010, four member states, Cape Verde,⁶⁰⁴ Burkina

⁶⁰⁴ *Law No. 133-V-2001 on the Protection of Personal Data*, enacted 22 January 2001, Cape Verde. This law established the initial comprehensive framework for data protection in Cape Verde and was the first of its kind in Africa.

Faso,⁶⁰⁵ Senegal,⁶⁰⁶ and Benin,⁶⁰⁷ had already developed their data protection legislation, which drew heavily from the French model. This early influence set a precedent that shaped subsequent laws in other member states, but it also raises important concerns about the extent to which African countries are developing legal frameworks that genuinely reflect their socio-cultural realities.

These early laws helped pave the way for the ECOWAS framework and set a legislative precedent that influenced subsequent laws in countries like Mali,⁶⁰⁸ Niger,⁶⁰⁹ and Togo,⁶¹⁰ which closely mirrored the provisions of the Supplementary Act. On the other hand, despite these developments, the regime of data protection within ECOWAS remains fragmented, with significant disparities in the implementation of national laws. For instance, three member states, Guinea, Guinea Bissau, and Liberia, still lack national data protection laws, creating debates over the enforceability of the ECOWAS framework in these countries.⁶¹¹ This uneven implementation highlights the challenge of creating a harmonized legal environment within ECOWAS, where the role of external models continues to shape legal developments in some countries, while others lag.

There is ongoing debate about whether ECOWAS laws should supersede national laws, as seen in the EU, or whether domestic legislation is necessary for these regional frameworks to

⁶⁰⁵ *Law No. 010-2004/AN on the Protection of Personal Data*, adopted 20 April 2004, Burkina Faso. This law established the legal framework for data protection in Burkina Faso, focusing on the rights of individuals and obligations of data handlers prior to the harmonization efforts by ECOWAS.

⁶⁰⁶ *Law No. 2008-12 on the Protection of Personal Data*, enacted 25 January 2008, Senegal. This law provides the framework for the protection of personal data within Senegal, establishing principles and guidelines for data processing and the rights of data subjects.

⁶⁰⁷ *Law No. 2009-09 on the Protection of Personal Data*, adopted 22 May 2009, Benin. This law established the legal framework for the protection of personal data in Benin, emphasizing the rights of individuals to control their personal information and setting standards for data processing and security.

⁶⁰⁸ *Law No. 2013-015 on the Protection of Personal Data*, 21 May 2013, Mali, available at <https://www.dataguidance.com/notes/mali-data-protection-overview> Accessed June 11, 2024.

⁶⁰⁹ *Law No. 2017-28 on the Protection of Personal Data*, 3 May 2017, Niger. This law outlines the regulations for handling personal data within Niger, including the roles and responsibilities of data controllers and processors.

⁶¹⁰ *Law No. 2019-014 on the Protection of Personal Data*, enacted on 29 October 2019, Togo. This law regulates the collection, processing, transmission, storage, and use of personal data, and also mandates the establishment of a data protection authority in Togo, although this has not yet been appointed.

⁶¹¹ Graham Greenleaf & Bertil Cottier, *supra* note 134.

be enforceable.⁶¹² This issue is particularly relevant in dualist states, where international treaties do not automatically become part of the national legal system without explicit legislative action. The patchwork implementation of data protection laws across ECOWAS reflects the complexity of harmonizing regional legal frameworks in a region where historical, linguistic, and political factors influence the adoption of laws. This challenge is further compounded by the influence of international models, raising questions about whether African states can assert greater control over the development of their legal systems or if they will continue to rely on external standards.

Article 48 of the ECOWAS Supplementary Act serves as a critical mechanism for operationalizing the provisions of the Act within member states. It establishes that for the provisions of the Act to become enforceable, they must be published in the country's national Official Journal. This requirement, while aiming to facilitate harmonization, also reflects the ongoing challenge of ensuring that regional frameworks are adequately implemented within national legal systems. As of June 2024, six member states have met this publication requirement, aligning their national laws accordingly.⁶¹³ However, even in these countries, the question remains whether the laws being implemented are truly reflective of local needs or if they are primarily influenced by external, particularly European, models. The context of these regulations within ECOWAS is also shaped by broader international efforts, such as the HIPSSA initiative, which was developed by the ITU and the EU. HIPSSA supports African countries in developing telecommunications laws that encompass data protection and cybercrime. While initiatives like HIPSSA aim to support African legal development, they often promote models that align with European standards, raising concerns about the extent

⁶¹² *Ibid.*

⁶¹³ *Ibid.*

to which these laws are adapted to Africa's unique digital realities.⁶¹⁴ The development of Model Laws through HIPSSA provides detailed guidance on the roles of data processors and sets rigorous standards for data handling, particularly in scientific research. Although these Model Laws offer valuable guidance, they are advisory rather than binding, further highlighting the tension between aligning with international standards and developing contextually relevant African frameworks.⁶¹⁵

While the ECOWAS Supplementary Act and initiatives like HIPSSA have been pivotal in setting a framework for data protection in West Africa, they focus heavily on aligning with international standards and encouraging high protection standards. This emphasis on international alignment reflects a broader trend of African legal frameworks being shaped by external models, raising critical questions about the ability of African states to assert their legal sovereignty in the realm of data protection. Moreover, the diversity of data protection laws within ECOWAS, and the varying degrees of implementation, further complicates the region's ability to create a truly harmonized legal framework. In contrast, the SADC offers a different spectrum of data protection laws, with countries like Angola and South Africa showing strong data protection regimes, while others are at varying stages of developing their frameworks. This variation within both ECOWAS and SADC highlights the broader challenge of developing regionally harmonized data protection laws that reflect local needs while avoiding the pitfalls of over-reliance on external legal models.

4.4.4 Data Protection and Privacy Laws in the Southern African Development Community (SADC): Influence of European Standards

The Southern African Development Community, comprising sixteen countries in southern and central Africa and several Indian Ocean states, presents a diverse framework of data

⁶¹⁴ International Telecommunication Union, "Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA)," available at <https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx>, accessed on June 13, 2024.

⁶¹⁵ *Ibid.*

protection and privacy laws. However, the extent to which these laws reflect African governance needs versus being shaped by external European standards raises critical questions about the legal sovereignty of SADC member states. Among the more advanced countries in the region, Angola,⁶¹⁶ South Africa,⁶¹⁷ Mauritius,⁶¹⁸ Eswatini,⁶¹⁹ and Tanzania⁶²⁰ have comprehensive data protection laws. These countries have made significant strides in implementing data protection frameworks, but their reliance on European legal models, particularly through the Model Law developed under the HIPSSA initiative, suggests a continued dependence on external legal standards.

In contrast, countries like Lesotho,⁶²¹ Madagascar,⁶²² and Seychelles⁶²³ have partial enforcement or limited data protections within their existing legal frameworks. This uneven implementation of data protection laws within SADC reveals the challenge of creating a harmonized regional approach, particularly when external models are relied upon rather than developing frameworks that reflect the unique socio-political contexts of SADC countries. Additionally, countries such as Mozambique, the Democratic Republic of Congo, Namibia, and Malawi are still in the process of developing their legal frameworks.⁶²⁴ This fragmented

⁶¹⁶ *Law No. 22/11 on the Protection of Personal Data*, enacted on 17 June 2011, Angola. This law establishes the framework for the collection, processing, and safeguarding of personal data within Angola.

⁶¹⁷ *Protection of Personal Information Act, 2013* (Act No. 4 of 2013), assented to on 19 November 2013, commenced on 1 July 2020, South Africa. This act sets the legal framework for the processing of personal information by public and private bodies, aiming to safeguard personal information and ensure data protection within the country.

⁶¹⁸ *Data Protection Act 2017* (Act No. 22 of 2017), enacted on 8 December 2017 and effective from 15 January 2018, Republic of Mauritius. The law includes provisions to align with the European Union's General Data Protection Regulation (GDPR) and establishes comprehensive data protection standards, overseen by the Mauritian Data Protection Office.

⁶¹⁹ *Data Protection Act, 2018* (Act No. 18 of 2018), assented to on 12 July 2018, Kingdom of Eswatini. This act provides for the protection of personal data processed by public and private bodies and establishes the Data Protection Authority for oversight and enforcement.

⁶²⁰ *Personal Data Protection Act, 2022* (Act No. 11 of 2022), enacted on 1 November 2022, effective from 1 May 2023, United Republic of Tanzania. This act sets the legal framework for the protection of personal data and establishes the Personal Data Protection Commission to ensure compliance and safeguard the privacy rights of individuals.

⁶²¹ *Data Protection Act 2011* (Act No. 5 of 2012), effective 22 February 2012, Kingdom of Lesotho.

⁶²² *Law No. 2014-038 on the Protection of Personal Data*, effective 21 January 2015, Republic of Madagascar.

⁶²³ *Data Protection Act 2003* (Act No. 9 of 2003), effective 1 March 2004, Republic of Seychelles.

⁶²⁴ HIPSSA Project," presentation slides hosted on Slideserve. Available online at <https://www.slideserve.com/toshi/hipssa-project>, accessed on June 13, 2024.

legal framework within SADC illustrates not only the diversity of approaches but also the varying levels of influence that European models exert on African legal development.

The HIPSSA Model Law, which has played a significant role in shaping the data protection regime across SADC, is a key driver of the region's alignment with European standards.⁶²⁵ While the HIPSSA initiative aims to harmonize data protection laws across sub-Saharan Africa, its reliance on European legal principles raises concerns about whether these frameworks truly address Africa's unique digital and governance challenges. The strategic alignment with European standards, facilitated through initiatives like HIPSSA, seeks to streamline data protection across national boundaries within SADC and sets the stage for broader regional coherence in how data protection is approached and enforced. However, this alignment also raises critical questions about whether African states are developing legal systems that are contextually relevant or if they are primarily adopting external norms that may not fully reflect the needs and realities of the region. In countries with more advanced data protection frameworks, such as South Africa, the influence of European standards is particularly evident in the Protection of Personal Information Act (POPIA),⁶²⁶ which mirrors key provisions of the European Union's GDPR. While the adoption of international best practices can facilitate cross-border data flows and enhance regulatory cooperation, it also risks overshadowing the development of African-centric legal frameworks that address the continent's unique socio-political and economic contexts. The question remains whether countries like South Africa, which have embraced European data protection standards, can develop a truly African approach to privacy or whether the legal systems they are adopting will continue to be shaped by external influences.

⁶²⁵ *Ibid.*

⁶²⁶ South Africa. Protection of Personal Information Act 4 of 2013. Government Gazette 37067, November 26, 2013.

The reliance on European models, particularly through the HIPSSA initiative, demonstrates the broader trend of legal harmonization in Africa being driven by external standards. This reliance raises critical concerns about the long-term sustainability of data protection frameworks that are not deeply rooted in African legal traditions and governance needs. While the goal of creating a harmonized legal landscape is important for regional cooperation and economic integration, it must be balanced with the need for these frameworks to reflect the unique challenges and opportunities of the African context.

4.4.5 Advancements in SADC Data Protection Legislation: HIPSSA Model Laws and European Influence

The HIPSSA initiative introduced model laws that have contributed to a sophisticated evolution in data protection legislation within the SADC. However, while these model laws represent a significant step forward in harmonizing regional data protection standards, their heavy reliance on EU norms raises critical concerns about whether they fully reflect Africa's unique digital landscape and governance needs. These laws, modelled closely on EU standards, particularly in their comprehensive approach to data protection, apply not only to data controllers based within a country but also to those operating outside the jurisdiction if they utilize processing means within the territory.⁶²⁷ This alignment with European legal principles, while providing a clear framework for data protection, also raises questions about the extent to which African states are developing legal frameworks that reflect their socio-political realities or merely adopting external models. One notable provision in these model laws is the requirement for data controllers to appoint a local representative if they process data within a territory, thus extending data protection across borders.⁶²⁸ While this requirement aims to protect African data subjects, it also mirrors the EU's approach,

⁶²⁷ SADC Model Law on Data Protection," International Telecommunication Union, available at https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf, accessed on June 13, 2024.

⁶²⁸ *Ibid.*

particularly as seen in the GDPR, raising further concerns about the reliance on external legal models. The organizational structure of the Data Protection Authority (DPA) within these model laws includes a diverse assembly of stakeholders such as judges, parliamentarians, and civil society representatives.⁶²⁹ This diversity is important for ensuring a broad perspective on data protection oversight, yet it remains to be seen whether this structure fully aligns with Africa's governance needs or reflects an attempt to replicate European governance models. The DPA's powers are also balanced by a parliamentary veto right, reinforcing legislative oversight and ensuring accountability.⁶³⁰ While this mechanism promotes checks and balances, its direct inspiration from European frameworks raises questions about whether this structure is adaptable to the unique political and legal systems of African countries.

The model laws also provide specific provisions for sensitive data types such as genetic, biometric, and health-related information, affording these data categories higher protection levels.⁶³¹ Although these provisions demonstrate an advanced understanding of the importance of sensitive data, the emphasis on protecting such data types follows global trends set by European standards, suggesting that the laws are more reflective of international priorities than of African-specific concerns. Data subjects are empowered with significant rights, including the right to be informed about the obligatory nature of data collection and the consequences of non-compliance.⁶³² However, the degree to which these rights are enforceable within African legal systems, where resource constraints and legal capacity vary significantly, remains a subject of critical analysis. Transparency rules are stringently applied when data is sourced from third parties, and in the event of a data breach, prompt notification to affected individuals is mandated.⁶³³ This mirrors the GDPR's approach to transparency and breach notification, but questions arise about whether African legal systems have the

⁶²⁹ *Ibid.*

⁶³⁰ *Ibid.*

⁶³¹ *Ibid.*

⁶³² *Ibid.*

⁶³³ *Ibid.*

infrastructure and resources to implement such rigorous standards effectively. Moreover, data controllers are required to demonstrate ongoing compliance with data protection norms, which enhances continuous adherence to privacy standards.⁶³⁴ This ongoing compliance mechanism, although beneficial, may place heavy administrative burdens on African companies and governments, potentially limiting the ability of local institutions to meet these standards.

Another key element of the model laws is the regulation of decisions made through automated processes. Data subjects are entitled to understand the logic involved in such decisions, particularly when it significantly impacts them personally.⁶³⁵ This provision reflects growing concerns about algorithmic transparency, a trend that originates from global digital governance debates but may not fully address the local realities and technological capacities within SADC countries. Similarly, any changes to data following an access request by a data subject must be communicated to all relevant third parties, maintaining a consistent and accountable data management chain.⁶³⁶ While this enhances transparency, it also mirrors European legal standards, raising questions about whether these measures are practical in the context of African legal and institutional capacity. Furthermore, a comprehensive legal framework governs the export of data, modelled closely on EU guidelines but with stricter controls on international data transfers.⁶³⁷ This cautious stance on global data exchanges reflects the concerns of European data protection models, particularly regarding data sovereignty, but it may not fully reflect the specific needs and capacities of African countries in managing cross-border data flows. While the intent to regulate international data transfers is important for protecting African data subjects, the question remains whether these stringent

⁶³⁴ *Ibid.*

⁶³⁵ *Ibid.*

⁶³⁶ *Ibid.*

⁶³⁷ *Ibid.*

controls are adaptable to the region's unique challenges or if they place undue restrictions on African businesses and governments seeking to engage in the global digital economy.

4.4.6 Data Protection Progress in the East African Community: EU Influence and Local Developments

The East African Community (EAC), which includes Kenya, Tanzania,⁶³⁸ Uganda, South Sudan, Rwanda, and Burundi, has made notable advancements in data protection legislation. However, these developments raise important questions about the extent to which local governance needs are being prioritized or whether the region's legal frameworks are overly influenced by EU standards, particularly the GDPR. In 2019, both Uganda⁶³⁹ and Kenya⁶⁴⁰ enacted data protection laws, with Kenya's legislation being particularly comprehensive. These laws closely mirror the principles of the GDPR, illustrating the EU's substantial impact on regional data privacy norms.⁶⁴¹ While the adoption of GDPR-like frameworks may enhance regulatory coherence and facilitate international data flows, it is critical to consider whether these frameworks are appropriately tailored to the unique socio-political contexts of East African countries. Rwanda⁶⁴² introduced its data protection law in 2021, followed by Tanzania⁶⁴³ in 2022, further demonstrating the region's commitment to aligning with global data protection trends. However, the influence of external models like

⁶³⁸ *East African Community (EAC)*, available online at <http://www.eac.int/> Accessed on June 13, 2024. Tanzania is a member of both the East African Community (EAC) and the Southern African Development Community (SADC).

⁶³⁹ *Data Protection and Privacy Act, 2019* (Act No. 9 of 2019), assented to on 25 February 2019, Uganda. This act regulates the collection and processing of personal data, establishes the rights of individuals to their data, and sets up the Office of the Data Protection Officer to oversee compliance.

⁶⁴⁰ *Data Protection Act, 2019* (Act No. 24 of 2019), assented to on 8 November 2019, Kenya. This law provides for the regulation of the processing of personal data, establishes the Office of the Data Protection Commissioner, and sets out the rights of data subjects and obligations of data controllers and processors.

⁶⁴¹ SecurityScorecard, "Countries With GDPR-Like Data Privacy Laws," blog post, available online at <https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws/>, accessed on June 13, 2024.

⁶⁴² *Law No. 058/2021 on the Protection of Personal Data and Privacy*, enacted on 13 October 2021 and officially gazetted on 15 October 2021, Republic of Rwanda. This law outlines regulations for personal data processing and establishes rights and obligations concerning data privacy.

⁶⁴³ *Personal Data Protection Act, 2019* (Act No. 9 of 2019), assented to on 1 November 2019, United Republic of Tanzania. This act establishes the legal framework for the protection of personal data, introduces the role of the Data Protection Commissioner, and sets out the rights of data subjects and obligations of data controllers and processors.

the GDPR raises concerns about whether African states are developing frameworks that reflect their own governance and socio-economic realities or simply replicating global standards without adequate contextualization.

Despite the progress seen in countries like Kenya and Rwanda, Burundi and South Sudan continue to lag, with no comprehensive data protection legislation currently in place. This uneven development across the region reflects broader challenges of legal harmonization in Africa, where external models may not always align with local needs. Nevertheless, the EAC has been actively encouraging its member states to enact data privacy legislation. The 2012 adoption of a Bill of Rights by the EAC legislature⁶⁴⁴ is a notable step forward, incorporating an explicit right to privacy, which is absent in the broader African Charter on Human and Peoples' Rights. However, the Bill of Rights has yet to be ratified by the EAC Heads of State, raising questions about the political will to fully integrate privacy protections within the region's legal frameworks. The inclusion of a right to legal enforcement, with the potential for appeals to the East African Court of Justice,⁶⁴⁵ is a significant development that could enhance the region's data protection regime once ratified. In addition to the Bill of Rights, the EAC has taken steps to support legal harmonization through the endorsement of the Frameworks for Cyberlaws Phases I and II, introduced in 2008 and 2011.⁶⁴⁶ While these frameworks address various aspects of cyber law, including data protection, the directives from Phase I are notably succinct, merely advocating for the adoption of international best practices. This reliance on external best practices, particularly those shaped by European legal standards, reflects the broader challenge of balancing global alignment with the need for local relevance in African legal systems.

⁶⁴⁴ *Bill of Rights*, adopted by the East African Legislative Assembly (EALA), 2012, East African Community. This legislative act aimed to ensure fundamental rights and freedoms within the member states of the EAC.

⁶⁴⁵ Alex B. Makulilo, "Myth and Reality of Harmonisation of Data Privacy Policies in Africa," *Computer Law and Security Review* 31, no. 1 (2015): 78-89.

⁶⁴⁶ *Ibid.*

Furthermore, in 2012, the EU/ITU's model law on data protection was specifically aimed at EAC countries, urging them to adopt comprehensive data protection statutes in line with this model.⁶⁴⁷ However, the question remains whether these model laws genuinely reflect the governance capacities and socio-political realities of East African countries or whether they are primarily driven by external influences. Unlike counterparts in SADC or ECCAS/CEMAC, the EAC has not yet adopted its model law, reflecting a more cautious approach to standardizing data protection across its member states. This caution may be interpreted as a recognition of the complexities involved in harmonizing laws within a region marked by significant socio-economic and political diversity, or it may reflect a hesitancy to adopt external models without careful consideration of their local applicability. As the EAC moves forward with data protection legislation that reflects EU influences, these laws must be adapted to address the unique challenges and opportunities within the region. The risk remains that without sufficient adaptation, the adoption of GDPR-like frameworks may entrench a dependency on external models, rather than fostering the development of truly African data protection regimes that are responsive to local needs.

Efforts to harmonize data protection laws across the African continent continue, with regions like the Economic Community of Central African States (ECCAS) and CEMAC also engaging with frameworks that incorporate both regional priorities and international standards. However, the ongoing challenge for African states will be to balance the benefits of global alignment with the imperative to develop legal frameworks that genuinely reflect African realities, promoting greater legal sovereignty and reducing dependency on external norms.

4.4.7 Data Protection Evolution in Central Africa: ECCAS and CEMAC's Model Laws

⁶⁴⁷ *Ibid.*

The ECCAS, comprising eleven predominantly French- and Portuguese-speaking countries, has seen notable advancements in data protection, though these developments raise important questions about the degree of external influence, particularly from European models, in shaping the region's data privacy frameworks. ECCAS works closely with the Association of Francophone Data Protection Authorities (AFAPDP), which plays a significant role in advocating for data privacy across its member states.⁶⁴⁸ This reliance on external bodies like the AFAPDP, which is itself influenced by European legal standards, suggests a continued trend of European influence in shaping Central Africa's data protection laws, raising concerns about whether these frameworks are sufficiently adapted to local governance needs. Additionally, the CEMAC, comprising six French-speaking countries, overlaps significantly with ECCAS members.⁶⁴⁹ Among these countries, Angola,⁶⁵⁰ Chad,⁶⁵¹ Gabon,⁶⁵² Equatorial Guinea,⁶⁵³ Sao Tome & Principe,⁶⁵⁴ and Congo-Brazzaville⁶⁵⁵ have enacted data privacy laws. However, the uneven development of data protection legislation across the region highlights broader challenges in harmonizing legal frameworks, particularly in regions where external models are predominant and may not fully reflect local socio-

⁶⁴⁸ Musoni, Melody, Poorva Karkare & Chloe Teevan. *Cross-border Data Flows in Africa: Continental Ambitions and Political Realities*, Discussion Paper No. 379, Maastricht: European Centre for Development Policy Management, 2024.

⁶⁴⁹ *Communauté Économique et Monétaire de l'Afrique Centrale* (CEMAC), established by the Treaty of N'Djamena, 16 March 1994, Central Africa. CEMAC aims to promote economic and financial integration among countries in the Central African region, including Cameroon, Central African Republic, Chad, Republic of Congo, Equatorial Guinea, and Gabon.

⁶⁵⁰ Law No. 22/11, Personal Data Protection Law, enacted on 17 June 2011, governs the processing of personal data and establishes the legal framework for data controllers and processors. The law is enforced by the Agência de Proteção de Dados (APD), which was established under Presidential Decree No. 214/16 of 10 October 2016.

⁶⁵¹ The data protection regime in Chad is governed by a comprehensive series of legislative acts and regulations, starting with Act No. 007/PR/2015 on Personal Data Protection, enacted on 10 February 2015. This was followed by Decree No. 075/PR/2019 on 21 January 2019, which implements the Act. Further legislative support includes Act No. 006/PR/2015, which established the National Agency for Computer Security and Electronic Certification, later amended by Ordinance No. 002/PR/2019, Ordinance No. 012/PT/2023 on 1 August 2023, Ordinance No. 014/PT/2023 on 30 August 2023, and Ordinance No. 009/PCMT/2022. Cybersecurity and cybercrime are addressed under Act No. 009/PR/2015 and Ordinance No. 008/PCMT/2022, while electronic transactions are regulated by Act No. 008/PR/2015.

⁶⁵² Law No. 1/2011 on Personal Data Protection in Gabon, enacted in January 2011, which addresses the processing and movement of personal data.

⁶⁵³ *Personal Data Protection Law No. 1/2016*, enacted on 22 July 2016.

⁶⁵⁴ *Law No. 03/2016 on the Protection of Personal Data*, only available in Portuguese.

⁶⁵⁵ *Law No. 29-2019 on the Protection of Data with a Personal Character*, enacted on 10 October 2019 and published in the official journal on 7 November 2019, entered into force on 25 November 2020.

political realities. Several ECCAS member states still lack comprehensive data protection laws, reflecting ongoing gaps in regional legal harmonization.

In a significant move toward regional standardization, ECCAS adopted three pivotal texts in 2013, which CEMAC also accepted as draft directives. These texts cover model laws on data protection, electronic communications, and cybercrime, reflecting an effort to create a unified approach to cyber regulation across Central Africa.⁶⁵⁶ While the adoption of these model laws is a positive step toward regional coherence, the question remains whether these frameworks, influenced by European standards, sufficiently address the unique legal, cultural, and socio-economic contexts of Central African countries. Notably, the ECCAS model law includes intricate details on genetic data in articles 6 and 7, reflecting a nuanced approach to sensitive data types. While this focus on sensitive data is commendable, it mirrors global trends in data protection shaped by European standards, raising questions about whether these provisions are tailored to the specific needs of Central African societies or if they are simply following global legal trends. Similarly, the CEMAC draft directive integrates provisions for civil compensation in cases of unlawful data processing, as outlined in Article 39. This provision for civil compensation illustrates an attempt to adapt data protection standards to the local context, but it is still heavily influenced by European models, reflecting the broader challenge of balancing external influences with the need for contextually relevant legal frameworks.

The evolution of data protection laws in Central Africa, particularly through ECCAS and CEMAC, demonstrates a commitment to aligning regional standards with global data protection trends. However, this alignment, particularly with European standards, risks overshadowing the development of truly African data protection regimes that are responsive

⁶⁵⁶ *ECCAS Model Law* was adopted as a model law, while the *Central African Economic and Monetary Community (CEMAC)* released the Draft Directives on Cybersecurity, Directive No. 07/08-UEAC-133-CM-18, in collaboration with the International Telecommunication Union (ITU).

to local governance needs. The region's reliance on external models, while beneficial in providing a clear regulatory framework, may entrench a dependency on foreign legal norms rather than fostering the development of autonomous, context-specific legal frameworks that reflect Central Africa's unique socio-political realities. Transitioning from Central Africa's approach to data privacy, the narrative shifts northward. Despite the lack of a specific sub-regional framework for data privacy in North Africa, countries like Tunisia⁶⁵⁷ and Morocco⁶⁵⁸ have demonstrated proactive engagement in aligning their legislative environments with global data protection standards. However, as with Central Africa, the challenge remains whether North African countries can develop data protection frameworks that balance global alignment with local relevance, promoting legal sovereignty while addressing the region's unique challenges.

4.4.8 Data Privacy Legislation and Influences in North Africa: Progress and Challenges

In North Africa, a region characterized by its location north of the Sahara, the development of data privacy frameworks presents both progress and challenges. Unlike sub-Saharan Africa, North Africa lacks a specific sub-regional organization devoted to data privacy. In this context, Tunisia⁶⁵⁹ and Morocco⁶⁶⁰ stand out for having established comprehensive data privacy laws and operational Data Protection Authorities. Both countries have undertaken significant reforms influenced heavily by the EU's GDPR, demonstrating a clear commitment to aligning with global data protection standards. However, this alignment

⁶⁵⁷ DLA Piper, "Data Protection Laws of the World: Tunisia," available at <https://www.dlapiperdataprotection.com/index.html?t=law&c=TN#:~:text=In%20this%20context%2C%20article%2030,the%20general%20rules%20of%20law>, accessed on June 12, 2024.

⁶⁵⁸ DLA Piper, "Data Protection Laws of the World: Morocco," available at <https://www.dlapiperdataprotection.com/index.html?t=law&c=MA&c2=>, accessed on June 12, 2024.

⁶⁵⁹ DLA Piper, "Data Protection Laws of the World: Tunisia," available at <https://www.dlapiperdataprotection.com/index.html?t=law&c=TN#:~:text=In%20this%20context%2C%20article%2030,the%20general%20rules%20of%20law>, accessed on June 12, 2024.

⁶⁶⁰ DLA Piper, "Data Protection Laws of the World: Morocco," available at <https://www.dlapiperdataprotection.com/index.html?t=law&c=MA&c2=>, accessed on June 12, 2024.

with the GDPR raises important questions about whether these frameworks, while enhancing global regulatory coherence, sufficiently address the specific governance needs and socio-political contexts of North Africa.

Since 2018, Tunisia has been actively working to overhaul its data protection framework, which was initially put in place before the democratic transformations following the Arab Spring.⁶⁶¹ These revisions, aimed at better reflecting democratic values, are heavily shaped by GDPR standards. While the alignment with European models may offer benefits in terms of regulatory coherence and international data flows, it remains unclear whether these standards are adaptable to Tunisia's evolving democratic system and the region's specific governance challenges. The influence of the GDPR, while ensuring compliance with global norms, risks overshadowing the development of frameworks that are more attuned to Tunisia's unique socio-political realities. Meanwhile, Algeria, despite introducing a data protection law in 2018, has faced criticism due to the law's lack of implementation and the absence of provisions for an independent Data Protection Authority.⁶⁶² This gap reflects broader challenges in the region, where the lack of effective institutional frameworks hinders the enforcement of data protection laws, potentially undermining citizens' privacy rights. The failure to establish an independent DPA not only limits the law's effectiveness but also signals deeper governance issues that must be addressed for Algeria to fully integrate into the global data protection landscape.

As North African countries like Tunisia and Morocco continue to update their data privacy laws, the pervasive influence of the GDPR highlights the significant external shaping force on their legal frameworks. While these countries are aligning closely with international norms, the ongoing question remains whether these frameworks are being tailored to address the democratic transformations and specific governance challenges within North Africa, or

⁶⁶¹ Masoud, Tarek, Jason Brownlee, and Andrew Reynolds. *The Arab Spring: Pathways of Repression and Reform*. Oxford University Press, 2015.

⁶⁶² Patricia Boshe, Moritz Hennemann & Ricarda von Meding, *supra* note 472.

whether they are simply following global trends without adequate contextualization. The heavy reliance on GDPR standards reflects a complex interplay between global standards and regional adaptations, but it also raises concerns about whether North African states are sufficiently developing autonomous legal frameworks that reflect their own socio-political needs.

4.5 Adapting Global Data Privacy Standards in Africa: European Influence and Regional Variability

The adaptation of data privacy laws within various African frameworks vividly demonstrates the significant influence of European models, particularly through the comparison of specific provisions related to data privacy. The GDPR has played a prominent role in shaping these frameworks, influencing the direction of data protection policies across African regions. However, this influence raises broader questions about whether these laws are being shaped by African states' local governance needs, or whether external pressures are driving compliance with international standards. For instance, in West Africa, the ECOWAS Supplementary Act of 2010 embeds key stipulations for lawful and fair data processing, as seen in Article 24, reflecting some degree of alignment with GDPR principles. While this alignment may enhance regulatory coherence and international engagement, it risks imposing a one-size-fits-all framework that may not fully address local socio-political realities. African states, in striving to meet global standards, may be adopting principles that do not always resonate with their own internal legal and cultural contexts. This can result in a tension where external frameworks dominate, leaving limited room for local innovation and contextual adaptation. In contrast, the AU Convention does not explicitly enumerate principles such as lawful data collection, which suggests that African states are not uniformly adopting global frameworks. This selective adaptation may indicate a cautious approach to external legal models, as countries weigh the benefits of global alignment against the need to retain legal

sovereignty. Even though principles like data quality, ensuring that data remains relevant, accurate, and current, are universally upheld across the continent, the broader question remains whether African legal systems are being shaped to fit global data flows or whether they are being designed to reflect the unique governance needs of African societies.

The principle of purpose specification, which mandates identifying the reasons for data collection at the time of acquisition, is another key aspect of GDPR that has influenced African data protection laws. This principle is reflected in Article 25(1) of the ECOWAS Supplementary Act and Article 13 of the SADC Model Law, but it is notably absent in the AU Convention. This omission raises the question of whether African frameworks are attempting to resist the wholesale adoption of foreign standards or if they are simply at different stages of legal evolution. In either case, it reveals the complex dynamic between aligning with international standards and addressing local governance priorities. The evolution of notifying data subjects about data collection purposes and their rights has become a major area of focus within African data protection laws, aligning closely with GDPR's disclosure requirements in Articles 13 and 14. However, it is important to ask whether these transparency measures reflect the specific needs of African societies or whether they are being adopted to fulfill the expectations of international actors, particularly those in Europe. African countries may face economic pressures to align with GDPR, as adherence to these standards can facilitate cross-border data flows and improve trade relations. Yet, the question remains whether such alignment fully serves the interests of African citizens or if it primarily serves global economic agendas.

Security measures to safeguard data are mandated across all African data protection instruments. Articles such as Article 28 of the ECOWAS Supplementary Act and similar provisions in the SADC Model Law demonstrate a clear commitment to secure data handling practices. While these provisions are crucial for data security, there is a deeper issue about

whether these security standards are being tailored to African realities or are being borrowed from external frameworks without sufficient localization. By closely following GDPR security requirements, African states may be prioritizing international acceptability over the development of a security regime that addresses their specific socio-political contexts. Additionally, the right of individuals to access and correct their data is a principle uniformly recognized across all African data protection instruments. This right fosters transparency and trust between data controllers and subjects, echoing similar provisions in the GDPR (Articles 15 and 16). However, there are concerns that this individual-focused right may not fully align with the communal and collective privacy norms prevalent in many African societies. By adopting standards that prioritize individual rights, African legal frameworks risk replicating a European legal ethos, potentially overlooking the need for more culturally attuned privacy protections. This shift towards individualism may undermine the broader collective and social aspects of privacy that are central to many African cultural practices.

Moreover, African data protection standards have seen significant development in alignment with GDPR principles. However, the process of legal adaptation across Africa is not merely a technical exercise, it is deeply political. The SADC Model Law, for example, aligns closely with GDPR standards, meeting key criteria that reflect global best practices. In contrast, the AU Convention and the ECOWAS Supplementary Act meet fewer of these criteria, reflecting their earlier establishment and the slower diffusion of GDPR principles across African regions. This disparity in alignment may also reflect a deliberate choice by some African states to retain greater legal flexibility and resist the full imposition of foreign standards. Ultimately, the reliance on GDPR reflects both Africa's engagement with global standards and the challenges African states face in asserting their legal sovereignty in a world where international norms are largely shaped by external powers. While aligning with these global standards can offer benefits in terms of trade and regulatory coherence, it also poses

the risk of sidelining African states' ability to develop context-specific frameworks that truly address their unique needs.

4.6 Conclusion

The analysis of data protection and privacy frameworks across Africa, particularly within the AU and its RECs, highlights both the progress made and the challenges that persist. Despite the efforts to develop continental frameworks, such as the AU Malabo Convention and the ECOWAS Supplementary Act, it is evident that these frameworks still lean heavily on European influences, particularly the GDPR, without sufficiently integrating Africa's unique socio-cultural and legal contexts. While the AU's Malabo Convention was intended to serve as a central pillar for harmonizing data protection laws across the continent, its impact has been limited. Few African countries have ratified the Convention, which reflects its struggle to gain traction across the diverse legal frameworks of the continent. The dual focus on both cybersecurity and data protection in the Convention may have contributed to conflicts in national policy implementation, reducing its efficacy. Moreover, the lack of a structured, continent-wide oversight body, akin to the European Data Protection Board, undermines consistent enforcement across African states, further diluting the Convention's potential influence.

More broadly, this chapter has demonstrated how African frameworks are profoundly shaped by external standards, especially from Europe, but they lack sufficient adaptation to African socio-cultural realities. Many of the privacy and data protection laws that have emerged in Africa mimic European standards, particularly the GDPR, yet they fail to reflect the continent's communal and collective privacy norms. This disconnect highlights a critical issue: the legal regimes adopted across the continent often prioritize alignment with global norms over addressing local governance needs. The emphasis on individual privacy rights, as seen in both the GDPR and AU's Malabo Convention, often contrasts with the collective

nature of privacy in African societies. This has resulted in frameworks that may be legally sound in a global context but struggle to resonate locally. This raises the fundamental question: Are African states truly developing data protection frameworks that reflect their cultural, social, and economic realities, or are they simply transplanting foreign models to meet global standards?

While regional initiatives within RECs such as ECOWAS, SADC, and ECCAS have made significant strides in harmonizing privacy and data protection laws, the lack of a coherent, Africa-centric approach remains a challenge. The absence of socio-cultural sensitivity within these frameworks suggests that Africa's emerging data governance architecture is still heavily dependent on external influences, particularly from Europe, rather than being a reflection of the continent's unique needs and priorities. It is clear from this analysis that Africa needs a socio-culturally sensitive approach to data protection. Rather than merely adopting European legal frameworks, Africa must focus on developing data protection regimes that take into account its communal values, economic realities, and legal traditions. The ambition to foster economic development and create a sustainable data-driven economy must be balanced with the need for culturally attuned legal frameworks that respect the collective nature of African societies. Looking ahead, the journey towards a comprehensive and effective data protection regime in Africa is ongoing. This chapter has highlighted the need for continued collaboration between African states, both regionally and continentally, to refine their legal frameworks in a way that addresses the unique socio-political contexts of the continent. African countries must strive not only to meet international data protection standards but also to carve out their path, one that reflects their cultural norms, governance realities, and developmental priorities. While the influence of European data protection standards is undeniable, the future of Africa's privacy and data protection framework must be shaped by African voices, perspectives, and values. This chapter calls for

a reimagining of the African data protection framework, one that is not only legally robust but also contextually relevant and capable of addressing the diverse needs of the continent's populations.

Chapter 5: Culturally Contextualizing Privacy and Data Protection: An African Approach to Regulation and Governance

5.0 Introduction

The importance of privacy and data protection in Africa parallels the rest of the world. However, as examined in Chapter 3, African countries encounter substantial hurdles in conforming to European privacy and data protection standards. While the GDPR has emerged as the global benchmark for privacy safeguards, its widespread adoption has provoked debate due to its perceived imperialistic undertones, which disregard the specific cultural and socioeconomic contexts of African countries.⁶⁶³ From a TWAIL perspective, this reflects ongoing digital colonialism, where African states are pressured to adopt Eurocentric legal models without adequate consideration of their local realities. TWAIL scholars argue that such global legal hierarchies sustain power imbalances that disadvantage the Global South. Scholars and organizations in these regions have challenged the EU's claim to be the sole arbiter of privacy and data protection norms, advocating for a more localized approach that reflects the indigenous values and realities of African societies.⁶⁶⁴ Despite calls for alternative models, no consolidated framework has been established. This gap highlights the need for a decolonized regulatory approach, which this thesis seeks to address. Consequently, this chapter addresses the third research question: How can privacy and data protection regulations be effectively tailored to Africa's unique cultural, social, and economic factors?

This chapter critiques the widespread imposition of Western legal frameworks in non-Western contexts, particularly the dominance of European data protection models that often

⁶⁶³ Manjoo, R., “*The Long Arm of GDPR in Africa: Reflection on Data Privacy Law Reform and Practice in Mauritius*” (2022) 14 Int'l J Law Info Tech 45.

⁶⁶⁴ Anand, S., & Ebras, D., “Data Colonialism: Rethinking Data Extraction and the Global South” Global Perspectives (2023).

overlook the unique socio-cultural and economic realities of African countries. Rather than uncritically adopting external standards, this chapter calls for a decolonized approach to privacy and data protection that aligns with African communal values, governance traditions, and economic structures. By examining alternative techniques that resonate with the African context, this chapter highlights the critical role of cultural norms and societal values in crafting effective regulations. It emphasizes the importance of integrating principles of collective ownership and communal stewardship into privacy and data protection policies, ensuring that frameworks resonate with the lived realities of African societies and address their specific challenges effectively.

To present a comprehensive analysis of these themes, this chapter is structured into six interconnected parts, each addressing how to tailor privacy and data protection concepts to the unique cultural, social, and economic setting of the region. It begins by analyzing existing privacy and data protection regulatory models, focusing on the GDPR, and the AU's Convention on Cybersecurity and Personal Data Protection. This is followed by an exploration of African cultural foundations and their implications for privacy regulation, highlighting the disconnect between Eurocentric privacy models and African societal values. The discussion then shifts to the development of a privacy and data protection framework that integrates African cultural values, emphasizing the need to balance individual rights with communal governance structures. Next, the chapter examines how African notions of communal ownership and custodianship can shape privacy and data protection laws that are both contextually relevant and reflective of traditional governance practices. This is complemented by a historical critique of how European colonial rule reshaped African customary laws and privacy frameworks, often imposing Eurocentric models that failed to account for African values. Finally, the chapter discusses the necessity of flexible regulatory approaches, proposing solutions such as open-source technologies and community-based

enforcement models to promote equitable and inclusive privacy and data protection governance across the continent. By focusing on these themes, this chapter aims to advance a contextually relevant, sovereignty-driven model of privacy and data protection regulation that aligns with Africa's socio-cultural realities while resisting external regulatory impositions.

5.1 Approaches to Regulation of privacy and data protection

Primarily, this thesis critically evaluates a range of regulatory frameworks for privacy and data protection, notably the GDPR, the AU's Convention on Cybersecurity and Personal Data Protection, and other regional and national frameworks within Africa. Each of these frameworks is implemented differently; the GDPR is uniformly enforced across EU member states, whereas the AU Convention necessitates adaptation and domestication within individual African countries,⁶⁶⁵ reflecting variances in legal, cultural, and socio-economic contexts. The academic discourse and legal analyses reveal three principal approaches to privacy and data protection. First, the individual rights-based approach empowers individuals with rights over their data, granting them substantial control over the collection, processing, and use of their information, while emphasizing personal autonomy and consent.⁶⁶⁶ Although widely regarded as the foundation of modern privacy laws, this model assumes a highly individualized notion of privacy, which may not fully resonate with African societies where communal structures often dictate privacy norms. In contrast, the traditional governance approach relies on the institutional role of governmental bodies in establishing and enforcing privacy standards.⁶⁶⁷ This often involves the creation of dedicated authorities tasked with overseeing data protection practices and ensuring compliance with statutory regulations, focusing on the structural and procedural aspects of data protection to institutionalize privacy

⁶⁶⁵ Abdulrauf, L.A., "The African Union's Data Protection Convention 2014: A Cause for Celebration of Human Rights in Africa?" (2014) 33-45.

⁶⁶⁶ Prinsloo, P. & Kaliisa, R., "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

⁶⁶⁷ Naidoo, J., "Namibia's Community-Based Natural Resource Management Program: The Politics of Communal Land Tenure and the Management of Local Natural Resources" (2011).

protections within public and private entities.⁶⁶⁸ However, in many African countries, resource constraints and institutional weaknesses may hinder the effective functioning of these oversight bodies, leading to inconsistent enforcement and a lack of regulatory legitimacy. Lastly, the regulation-based approach emphasizes the codification of privacy standards into specific laws and regulations that delineate acceptable practices for data handling.⁶⁶⁹ These regulations provide clear guidelines for entities on data collection, storage, and processing, aiming to create a comprehensive legal framework that entities must follow to ensure data protection. Yet, the mere codification of laws without adequate contextualization may result in frameworks that exist in the legal text but fail in practical implementation, particularly when modelled after European legal traditions that do not align with Africa's socio-economic structures.

The legal frameworks examined in Chapter 4, including the GDPR, the AU Convention, various African model laws, and national legislation, encapsulate differing approaches to privacy and data protection. These frameworks represent a synthesis of diverse regulatory strategies, demonstrating a comprehensive methodology that strives to balance individual rights with institutional accountability and well-defined legal standards. However, a critical analysis of these frameworks reveals an essential challenge: while structured regulatory approaches lay the groundwork for data protection, their success is often contingent on their adaptability to local cultural, economic, and societal conditions. The application of the GDPR within African jurisdictions, for instance, presents distinct challenges, as its European-centric origins frequently clash with African communal values and societal structures.⁶⁷⁰ TWAIL scholars highlight this as an instance of regulatory imperialism, where African states are subjected to external legal paradigms that reinforce

⁶⁶⁸ Solove, Daniel. "The Three General Approaches to Privacy Regulation" *Teach Privacy*, 2020. Online: <https://teachprivacy.com/the-three-general-approaches-to-privacy-regulation/>, accessed September 2, 2024.

⁶⁶⁹ Ibid.

⁶⁷⁰ Anand & Ebras, *supra* note 666.

global power asymmetries. Compliance with European data protection norms often becomes a prerequisite for participation in international trade and economic relations, creating a scenario where African legal sovereignty is compromised.

The imposition of European standards such as the GDPR on African countries reflects a broader pattern of international legal frameworks perpetuating unequal global power relations.⁶⁷¹ This is evident in the way African states are pressured to harmonize their laws with European standards, not necessarily because these models are optimal for African societies, but because non-compliance carries economic costs. African states, frequently under economic and political pressure to conform to these frameworks as a condition for engaging in international trade and political relationships, encounter significant obstacles in modifying these models to suit their local realities. This external pressure not only challenges the adaptability of these frameworks but also undermines the development of African-centered regulatory models that prioritize indigenous governance traditions and local economic needs.⁶⁷² Consequently, the persistent economic and legal dependence on the Global North exacerbates the challenges African countries face in developing contextually relevant legal frameworks. Amidst these challenges, initiatives like the AfCFTA Protocol on Digital Trade offer a promising alternative, presenting an opportunity for African states to take ownership of their data governance regimes by fostering a continental approach that is responsive to African economic, legal, and technological realities. Similarly, the implementation of the AU Convention highlights the need for legal frameworks that are both legally sound and culturally aligned, capable of adapting to the diverse realities across African societies.⁶⁷³ Without a shift toward legal frameworks that reflect African

⁶⁷¹ Ibid.

⁶⁷² Cobbah, J. A. M., “*African Values and the Human Rights Debate: An African Perspective*” (1987), *Human Rights Quarterly* 9(3): 309–331.

⁶⁷³ Abdulrauf, L.A, *supra* note 667, “The African Union’s Data Protection Convention 2014: A Cause for Celebration of Human Rights in Africa?” (2014), at 33–45.

epistemologies and governance traditions, regulatory policies risk remaining externally dictated, reinforcing historical patterns of legal dependence.

Thus, there is a clear need for regulatory frameworks that are not only comprehensive and multifaceted but also flexible enough to be tailored to the diverse cultural, societal, and economic contexts of different regions. Such frameworks should be designed to enforce compliance while simultaneously fostering a contextually relevant understanding of privacy and data protection, ensuring that legal frameworks are not merely transplants from the Global North but rather products of African legal thought and economic priorities. This approach is critical for the development of effective, locally sustainable legal frameworks that respect both global standards and regional nuances.

5.1.1 Individual Rights-Based Approach to Privacy and Data Protection

The individual rights-based approach to privacy protection is fundamentally centred on providing individuals with extensive control over their data through a structured set of rights, predominantly anchored in the principle of consent.⁶⁷⁴ This consent serves as the legal basis for various forms of data collection, usage, and disclosure, enabling individuals to make informed decisions regarding their personal information. The GDPR, particularly in Chapter 3, clearly delineates these rights, emphasizing the significance of transparency, effective communication, and clear mechanisms for exercising data subject rights.⁶⁷⁵ For example, Article 12 of the GDPR requires data controllers to present information in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.⁶⁷⁶ This information must be provided in writing, electronically, or orally, provided that the data

⁶⁷⁴ Solove, Daniel, *supra* note 670, “The Three General Approaches to Privacy Regulation” Teach Privacy, 2020, available online: <https://teachprivacy.com/the-three-general-approaches-to-privacy-regulation/>, accessed September 2, 2024.

⁶⁷⁵ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

⁶⁷⁶ GDPR Art. 12, “Transparent information, communication and modalities for the exercise of the rights of the data subject.”

subject's identity is verified. The framework extends beyond merely establishing individual rights, as it also delineates the obligations of data controllers to actively facilitate the exercise of these rights, as outlined in Articles 15 to 22 of the GDPR. However, scholars such as Daniel J. Solove critique this model for failing to provide individuals with meaningful control over their data.⁶⁷⁷ The complexity of modern digital structures, where multiple entities process personal data, creates cognitive and structural challenges that undermine the effectiveness of consent mechanisms.⁶⁷⁸ Similarly, Neil Richards,⁶⁷⁹ Julie Cohen,⁶⁸⁰ and Lior Strahilevitz⁶⁸¹ argue that privacy serves broader social functions beyond individual control, supporting intellectual exploration, innovation, and maintaining social equity.

While the individual rights-based approach reinforces data subject autonomy and enhances operational transparency, it raises significant challenges in implementation, particularly across diverse socio-economic contexts such as those found in Africa. To illustrate how these challenges are being addressed, a pertinent example of an African country attempting to navigate this complexity is Kenya's Data Protection Act (2019). Although inspired by the GDPR, Kenya's legislation incorporates provisions tailored to its unique socio-economic landscape, such as a flexible approach to data localization.⁶⁸² For instance, the Act allows for the cross-border transfer of data, provided the receiving country implements adequate data protection measures. This provision reflects an attempt to balance competing priorities. It recognizes Kenya's reliance on international data flows for trade, while simultaneously seeking to uphold national sovereignty.

Similarly, South Africa's POPIA seeks to balance international standards with local realities by incorporating specific protections for biometric data and sensitive personal

⁶⁷⁷Solove, D.J., "*Privacy Self-Management and the Consent Dilemma*" (2013) 126 Harv L Rev 1880.

⁶⁷⁸ *Ibid.*

⁶⁷⁹ Neil M Richards, "The Dangers of Surveillance" (2013) 126 Harv L Rev 1945 at 1945-52.

⁶⁸⁰ Julie E Cohen, "What Privacy Is For" (2013) 126 Harv L Rev 1904 at 1918-27.

⁶⁸¹ Lior Jacob Strahilevitz, "Toward a Positive Theory of Privacy Law" (2013) 126 Harv L Rev 2010.

⁶⁸² Kenya Data Protection Act 2019, Section 48(2).

information.⁶⁸³ These safeguards are particularly pertinent given South Africa's historical context of state surveillance during apartheid. Both Kenya and South Africa's frameworks demonstrate how African countries are localizing international data protection norms to better reflect their unique socio-economic, cultural, and historical contexts. Nonetheless, despite these legislative efforts, challenges persist in ensuring that these frameworks align with the deeply embedded communal values of African societies. The practical difficulties of implementing these frameworks, particularly in rural or resource-constrained areas, further complicate the situation. In Kenya, for example, the full implementation of the Data Protection Act has been hampered by limitations in digital infrastructure, particularly in rural regions where the technology required for compliance is lacking.⁶⁸⁴ This brings into focus the reality that, even when local laws are enacted, their effective implementation depends on careful adaptation to the specific conditions and capacities of local contexts. For instance, Rwanda presents a more recent case of digital governance efforts within the African context.

Notably, Rwanda has emerged as a leader in digital transformation on the continent, and in 2021, it introduced a data protection and privacy law that aims to strike a balance between local realities and global standards.⁶⁸⁵ The law imposes detailed obligations on data controllers and processors while considering Rwanda's specific technological infrastructure, particularly the widespread use of mobile technology in rural areas.⁶⁸⁶ Despite these progressive legislative efforts, Rwanda continues to face challenges with enforcement, particularly in rural areas where technological literacy is low and resource limitations remain

⁶⁸³ South Africa, *Protection of Personal Information Act*, 2013 (Act 4 of 2013), ss 1 (definition of "biometrics"), 26, 27 (special personal information / biometrics).

⁶⁸⁴ Alunge, R., "*The Effect of Africa's Adoption of the EU Notion of Personal Data: The Case of Examination Results*" (2019), IST-Africa Conf Proc, 1-13.

⁶⁸⁵ Rwanda, *Law No. 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy*, Official Gazette, No. 42 of 18 October 2021.

⁶⁸⁶ Ibid.

a significant hurdle.⁶⁸⁷ Similarly, Kenya's Data Protection Act, while forward-thinking in its scope, has encountered difficulties in achieving widespread implementation due to similar infrastructural constraints.⁶⁸⁸ The Kenya Data Protection Commissioner has noted that many rural areas lack the digital literacy necessary to fully engage with the Act's provisions, resulting in enforcement efforts being concentrated predominantly in urban centers.⁶⁸⁹ These case studies reveal the ongoing tension between the aspirations of progressive legal frameworks and the practical realities of technology infrastructure and local capacity for engagement.

Building on these implementation realities, in African contexts the effectiveness of consent as an individual right, particularly where data implicate more than one person such as family or community information, is often limited by uneven digital literacy, constrained access to information, and communal patterns of decision-making. These conditions show that the Western conception of individual consent, premised on personal autonomy and informed choice, does not always align with local social realities in such settings. Relational consent offers a more contextually grounded alternative: it does not displace individual autonomy but supplements it by recognizing that personal-data decisions are shaped by kinship, community norms, and collective welfare. Accordingly, in these circumstances, consent is better understood as a socially negotiated process rather than a purely individual declaration.

⁶⁸⁷ See Rwanda's data governance: Navigating data governance in the public sector, *Brookings* (2021), online: <https://www.brookings.edu/articles/rwandas-data-governance-navigating-data-governance-in-the-public-sector/>, accessed September 5, 2024.

⁶⁸⁸ Oscar M. Otele, "Kenya's Data Protection Regime: Challenges and Future Prospects" (2021) 1 *Journal of African Politics* 66-88.

⁶⁸⁹ Kenya Institute for Public Policy Research and Analysis (KIPPRA), "Strengthening Data Protection in Kenya: Opportunities and the Way Forward" (30 March 2022), online: KIPPRA <https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/>, accessed September 5, 2024.

While the GDPR and similar standards are often presented as universal models, they do not always align neatly with non-Western contexts.⁶⁹⁰ In African societies, privacy considerations frequently extend into communal spaces, necessitating frameworks that recognize collective data governance practices. The AU and RECs have attempted to harmonize these standards with the EU model, but as discussed in previous chapters, significant disparities remain.⁶⁹¹ Thus, while the individual rights-based approach remains a foundational pillar of contemporary data protection strategies globally, its direct transplantation into African contexts necessitates critical re-evaluation. Instead, privacy and data protection frameworks must account for local cultural and societal norms, ensuring that regulations balance both individual and collective rights. This approach acknowledges the legitimacy of community-based privacy norms while also safeguarding individuals within rapidly digitizing African economies.

5.1.2 Traditional Governance Approach to Privacy Regulation

The traditional governance approach to privacy regulation mandates a comprehensive set of requirements to ensure robust data protection, emphasizing the importance of structural mechanisms within organizations.⁶⁹² This model includes mandatory roles such as a chief privacy officer or data protection officer, routine risk audits, and the implementation of detailed policies and procedures.⁶⁹³ These requirements are designed to systematize privacy and data protection compliance across organizations, addressing the operational aspects of privacy management. However, while these measures aim to strengthen privacy governance, they often assume a legal and institutional infrastructure that may not be universally

⁶⁹⁰ Cara Mannion, “Data Imperialism: The GDPR’s Disastrous Impact on Africa’s E-Commerce Markets” (2020) 53 *Vanderbilt Journal of Transnational Law* 685-710.

⁶⁹¹ Abdulrauf, L.A., *supra* note 667, “The African Union’s Data Protection Convention 2014: A Cause for Celebration of Human Rights in Africa?” (2014), at 33-45.

⁶⁹² Alunge, R., *supra* note 686, “The Effect of Africa’s Adoption of the EU Notion of Personal Data: The Case of Examination Results” (2019), IST-Africa Conf Proc, at 1-13.

⁶⁹³ Regulation (EU) 2016/679 (General Data Protection Regulation), Article 37.

available, particularly in regions with developing regulatory capacities. The GDPR exemplifies this traditional governance approach. It not only provides significant rights to data subjects but also establishes a structured governance framework essential for the enforcement of these rights.⁶⁹⁴ This is evident in the GDPR's detailed provisions starting from Article 51, which requires EU member states to establish independent supervisory authorities responsible for monitoring the application of the GDPR.⁶⁹⁵ These authorities are pivotal in ensuring the protection of individuals' fundamental rights and facilitating the free flow of personal data within the EU.

Additionally, Articles 52 and 53 further reinforce the independence and qualifications required for members of these supervisory authorities, emphasizing that they must act without external influence and engage in tasks and powers with appropriate resources provided by member states. Moreover, the operational aspects, such as conducting privacy impact assessments and engaging in privacy by design as outlined in the GDPR, illustrate this approach's emphasis on governance through detailed procedural compliance.⁶⁹⁶ However, this compliance-centric model often prioritizes formal adherence to privacy and data protection policies rather than ensuring meaningful protection of data subjects. Scholars like Ari Waldman⁶⁹⁷ critique this approach, arguing that the apparent comprehensiveness of such privacy laws can be misleading. Waldman suggests that these laws often fail to deliver actual protection, turning privacy compliance into a checkbox exercise that prioritizes managerial interests over substantive privacy rights.⁶⁹⁸ Waldman's critique is echoed by Julie Cohen, who notes that the managerial approach to privacy often emphasizes efficiency and

⁶⁹⁴ Waldman, A., *Privacy as Trust: Information Privacy for an Information Age* (2018), Cambridge University Press.

⁶⁹⁵ GDPR Art. 51, "Supervisory Authorities", Regulation (EU) 2016/679.

⁶⁹⁶ Cavoukian, A., *Privacy by Design: The 7 Foundational Principles* (2011), Information and Privacy Commissioner of Ontario.

⁶⁹⁷ Waldman, A., *supra* note 696, *Privacy as Trust: Information Privacy for an Information Age* (2018), Cambridge University Press.

⁶⁹⁸ Waldman, A., "Privacy Law as Checkbox Compliance" (2018) 14(2) Journal of Law & Policy 147.

innovation at the expense of robust privacy protections.⁶⁹⁹ This critique aligns with concerns raised in TWAIL scholarship, which argues that legal frameworks imposed from the Global North tend to privilege corporate and bureaucratic interests over the lived experiences of individuals in the Global South.

In the African context, the adoption of such a governance framework faces unique challenges, particularly due to resource limitations, regulatory capacity gaps, and socio-economic realities that differ significantly from the EU model.⁷⁰⁰ The enforcement mechanisms and supervisory authorities as prescribed might not be entirely effective if institutions lack the autonomy, financial resources, or technical expertise required to enforce compliance. The AU's Convention on Cybersecurity and Personal Data Protection attempts to mirror some of these governance structures but requires domestication to align with local realities,⁷⁰¹ illustrating the challenge of transplanting governance models that do not fully account for African regulatory and socio-political conditions. The dominance of the European governance model in privacy regulation also reflects broader global asymmetries in data governance. TWAIL scholars argue that international standards disproportionately favor Global North jurisdictions, reinforcing a regulatory order that often marginalizes African states' capacity to develop indigenous legal frameworks. This reveals that while the traditional governance approach provides a structured framework for managing privacy and data protection, it cannot operate in isolation, particularly in African contexts where regulatory effectiveness depends on a combination of legal, institutional, and socio-cultural factors.⁷⁰² Thus, it is critical to develop a privacy governance model that goes beyond procedural compliance and embodies substantive rights while reflecting the unique cultural

⁶⁹⁹ Cohen, J.E., *"What Privacy is For"* (2013) 126 Harv L Rev 1904.

⁷⁰⁰ Naidoo, J., *supra* note 669, "Namibia's Community-Based Natural Resource Management Program: The Politics of Communal Land Tenure and the Management of Local Natural Resources" (2011).

⁷⁰¹ Abdulrauf, L.A., *supra* note 667, "The African Union's Data Protection Convention 2014: A Cause for Celebration of Human Rights in Africa?" (2014), at 33-45.

⁷⁰² Owoniyi, S., *"African Cultural Values: The Past, Present and Future"* at 1-23.

and economic contexts of African societies. This is especially important in regions like Africa, where communal values and socio-cultural nuances shape how privacy is understood and exercised. A more context-sensitive approach would ensure that privacy and data protection regulations are not only legally enforceable but also practically viable and socially embedded.⁷⁰³

5.1.3 The Regulation Approach to privacy and data protection

The regulation approach to privacy, which focuses on substantively regulating the uses of personal data, presents a more effective means of ensuring data protection compared to other methods.⁷⁰⁴ The individual rights-based approach places the onus on individuals to manage their privacy, assuming that if companies provide certain rights, individuals will adequately protect their data.⁷⁰⁵ However, this assumption has been widely criticized for placing an unrealistic burden on individuals, given the complexity of modern data frameworks and the power imbalances between data subjects and corporate entities. As a result, this approach often fails to provide meaningful privacy protection, particularly in contexts where digital literacy levels are low or where structural barriers limit individuals' ability to exercise their rights. Similarly, the traditional governance approach, which emphasizes organizational processes, tends to prioritize procedural compliance over substantive privacy safeguards.⁷⁰⁶ While this approach mandates the appointment of privacy officers, the conduct of privacy impact assessments, and the implementation of policies and procedures, it frequently lacks enforceable substantive requirements for privacy and data

⁷⁰³ Prinsloo, P. & Kaliisa, R., *supra* note 668, "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

⁷⁰⁴ Waldman, A., *supra* note 700, "Privacy Law as Checkbox Compliance" (2018) 14(2) *Journal of Law & Policy* 147.

⁷⁰⁵ Solove, D.J., "Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880.

⁷⁰⁶ Prinsloo, P. & Kaliisa, R., *supra* note 668, "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

protection.⁷⁰⁷ As a result, organizations may fulfill these procedural requirements without genuinely enhancing privacy and data protection, thereby reducing governance compliance to a formalistic exercise rather than a substantive privacy and data protection framework.

In contrast, the regulation approach imposes substantive restrictions on how personal information can be utilized.⁷⁰⁸ This method is evident in various national and regional legislations, as explored in Chapter 4 of this thesis. Under this model, laws explicitly define permissible uses of personal data while prohibiting unauthorized uses, thus providing a clearer framework for compliance. Although this approach introduces stronger privacy protections, it also has its limitations. For instance, the GDPR in the EU requires justifications for using personal data, known as lawful bases.⁷⁰⁹ However, some of these lawful bases, such as legitimate interests, are broadly defined, granting companies considerable discretion on how they use personal data. This broad discretion creates a loophole that can undermine the regulation's intent to provide substantive privacy protections.⁷¹⁰ Furthermore, the GDPR encourages the principle of privacy by design, which advocates for integrating privacy considerations into the development of products and services from the outset.⁷¹¹ Despite this principle, the regulation offers minimal guidance on what it means to design for privacy. The concept of privacy, or data protection as referred to in the GDPR, is complex and subjective. The effectiveness of designing for privacy hinges on one's understanding of what constitutes privacy, which can vary significantly. Often, organizations adopt a narrow view of privacy, focusing on limited aspects rather than a

⁷⁰⁷ GDPR Art. 35, “*Data Protection Impact Assessments*”, Regulation (EU) 2016/679.

⁷⁰⁸ Cavoukian, A., *supra* note 707, “Privacy by Design: The 7 Foundational Principles” (2011), Information and Privacy Commissioner of Ontario.

⁷⁰⁹ GDPR Art. 6, “*Lawfulness of Processing*”, Regulation (EU) 2016/679.

⁷¹⁰ Waldman, A., *supra* note 700, “Privacy Law as Checkbox Compliance” (2018) 14(2) *Journal of Law & Policy* 147.

⁷¹¹ 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), *OJ L 119*, 4 May 2016, p. 1.

comprehensive protection framework.⁷¹² Addressing privacy through design choices involves substantive issues that are not adequately covered by the GDPR. A central reason the GDPR sits uneasily in many African settings is its basic orientation toward the individual as the primary unit of analysis. In many African contexts, personhood is constituted relationally through kinship, lineage, and community membership. This divergence surfaces in three linked pressure points. First, identity: Recital 34 conceptualizes genetic and identity-related data in individual, biomedical terms; yet information about one person may also implicate family, clan, or lineage, so the privacy interest is partly collective. Second, sensitivity and harm: building on that relational identity, Recital 51 frames special categories to protect individuals from discrimination, but disclosure of attributes such as health status, ethnic affiliation, or genetic disorders can generate stigma and reputational injury borne by households or communities making sensitivity relational as well as individual. Third, consent: in light of these relational stakes, Article 4(11)'s model of consent as a discrete, individual act often fails to reflect decision-making that, in practice, is consulted or negotiated through familial or communal structures; this does not negate individual agency but supplements it while preserving the individual's ability to object or withdraw. Taken together, these linked dynamics show why a strictly individual-rights model risks misdescribing practice; absent contextual adaptation, transplantation can yield conceptual and operational misalignment.

Similarly, the regulation approach, while offering a more substantial framework than the individual rights-based or governance approaches, still falls short in addressing the unique socio-economic and cultural contexts of regions like Africa.⁷¹³ The assumption that uniform regulatory models can be effectively transplanted into diverse legal environments overlooks

⁷¹² Cavoukian, A., *supra* note 698, "Privacy by Design: The 7 Foundational Principles" (2011), Information and Privacy Commissioner of Ontario.

⁷¹³ Alunge, R., *supra* note 686, "The Effect of Africa's Adoption of the EU Notion of Personal Data: The Case of Examination Results" (2019), IST-Africa Conf Proc, at 1-13.

the fact that privacy norms vary significantly across jurisdictions. From a TWAIL perspective, the global dominance of European regulatory models in data protection reflects deeper power asymmetries in international law, where African states are frequently pressured to adopt externally crafted regulations with minimal consideration for local realities. African countries' privacy and data protection frameworks should be tailored to their specific legal traditions, economic structures, and governance challenges. For example, rigid regulatory obligations that require extensive compliance mechanisms may not be feasible in jurisdictions with limited regulatory resources. A one-size-fits-all approach, such as that provided by the GDPR, often does not align with the regulatory and institutional capacities of many African nations.⁷¹⁴ Despite its provision of more substantive privacy protections, the regulation approach faces significant challenges in implementation, enforcement, and adaptability. To achieve effective privacy and data protection in diverse legal and cultural environments such as Africa, it is essential to develop contextually grounded regulations that not only align with global best practices but also reflect indigenous privacy norms and governance structures. References here to indigenous, cultural, or communal data serve to contextualize African data-sovereignty concerns; they are not advanced as falling within the GDPR's personal-data regime, except where such information constitutes personal data. A successful regulatory model for Africa must integrate substantive privacy safeguards with flexible, locally adapted enforcement mechanisms that acknowledge socio-economic disparities and technological limitations.

5.1.4 Culturally Contextual approach to privacy and data protection

The three predominant frameworks governing privacy and data protection, the individual rights-based, traditional governance, and use of regulation, demonstrate significant

⁷¹⁴ Prinsloo, P. & Kaliisa, R., *supra* note 668, "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

limitations when applied within the African context. The GDPR, which synthesizes these models, is frequently critiqued for perpetuating neocolonial tendencies.⁷¹⁵ This critique arises from the GDPR's development without adequate consideration for the distinct socio-economic and cultural realities of African countries, rendering its direct application in Africa both unsuitable and ineffective.⁷¹⁶ This thesis advocates for a culturally contextual approach to privacy and data protection, one that diverges from Eurocentric norms and is deeply embedded in local realities. Central to this approach is the principle of contextualization, acknowledging Africa's diverse cultural, social, and economic realities.⁷¹⁷ This principle highlights the necessity of adapting privacy and data protection frameworks to align with the unique needs and values of African communities. Despite the GDPR's de facto status as a global standard, it frequently fails to address specific African challenges, as extensively discussed in previous chapters, particularly Chapter 3. The rigid, universal application of such standards does not account for the continent's varied contexts, necessitating a more nuanced and localized regulatory approach to ensure both the effectiveness and legitimacy of privacy laws within Africa. Adopting a decolonial perspective is pivotal in addressing the continent's economic and technological disparities.⁷¹⁸ Uniform data protection regulations can be particularly challenging in resource-constrained environments, where the digital divide and infrastructural deficits hinder effective implementation. Contextually adapted frameworks, which are both flexible and scalable, are thus essential. They cater to the diverse socio-economic realities of different African countries and communities, ensuring that data protection measures resonate with local needs and conditions.⁷¹⁹

⁷¹⁵ Mannion, C., *supra* note 692, "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets" (2020) 53 *Vanderbilt Journal of Transnational Law* 685-710.

⁷¹⁶ *Ibid.*

⁷¹⁷ Abdulrauf, L.A., *supra* note 703, "The African Union's Data Protection Convention 2014: A Cause for Celebration of Human Rights in Africa?" (2014), at 33-45.

⁷¹⁸ Anand, S. & Ebras, D., *supra* note 666, "Data Colonialism: Rethinking Data Extraction and the Global South" *Global Perspectives* (2023).

⁷¹⁹ Prinsloo, P. & Kaliisa, R., *supra* note 668, "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

While the culturally contextual approach emphasizes individual and collective dimensions, it is equally important to consider the dynamics of inter-communal relationships within African societies. These dynamics, shaped by historical, cultural, and social ties, influence how privacy is perceived, negotiated, and protected across different communities. In many African societies, inter-communal relationships are governed by shared resources, traditional conflict resolution mechanisms, and collective decision-making.⁷²⁰ These relationships often require balancing privacy with the necessity for openness and mutual accountability among communities. For example, data about communal land or shared cultural artifacts may involve overlapping claims of ownership, making privacy a negotiated concept rather than an individualistic one.⁷²¹ This inter-communal lens necessitates a framework that not only respects individual and community privacy but also fosters collaboration and trust between communities. Such a framework would account for the fluid boundaries of privacy in contexts where interdependence is a cultural norm, ensuring that data governance mechanisms address cross-community data sharing and collective ownership. Incorporating inter-communal dynamics into privacy and data protection frameworks ensures that policies are reflective of Africa's collective cultural ethos.

Effective privacy and data protection frameworks in Africa also demand a strong emphasis on community engagement and participatory methods.⁷²² Such an approach involves active dialogue and collaboration with a broad spectrum of stakeholders, including traditional leaders, civil society organizations, and end-users. This engagement ensures that the formulation of data governance models is profoundly influenced by the cultural and social

⁷²⁰ Cobbah, Josiah A. M. "African Values and the Human Rights Debate: An African Perspective." *Human Rights Quarterly* 9, no. 3 (1987): 309–331.

⁷²¹ Naidoo, J, "Namibia's Community-Based Natural Resource Management Program: The Politics of Communal Land Tenure and the Management of Local Natural Resources" (2011) 57:1 *Africa Today* 69–84, online (JSTOR): <https://www.jstor.org/stable/44519300>, accessed 10 September 2024.

⁷²² Ibid.

dynamics that shape local perceptions of privacy.⁷²³ This inclusive, community-centric approach not only fosters the promotion of digital rights and trust within the digital ecosystem but also ensures that data protection measures reflect the aspirations and lived experiences of African societies. Ultimately, acknowledging the inherently collective nature of many African societies, it becomes imperative to weave local values, norms, and practices into data governance frameworks, thus enhancing their relevance and effectiveness in the African context.

The influence of the GDPR remains significant, particularly in its stringent third-party data processing requirements and economic impacts on non-EU countries. This external pressure has often led African countries to adopt legislative frameworks modelled on the GDPR, frequently without adequate adaptation to local contexts.⁷²⁴ While some modifications have been made, privacy and data protection legislative frameworks across Africa often remain overly reliant on EU standards, which may not suit the unique African context. The culturally contextual approach necessitates an exploration of the cultural anthropology of privacy, recognizing the multifaceted nature of privacy concerns. Scholars categorize privacy rights into four key areas:⁷²⁵ territorial privacy, which involves authority over one's physical space; bodily privacy, which relates to autonomy over one's body; informational privacy, which concerns control over personal information; and communications privacy, which protects the security and confidentiality of communications.⁷²⁶

⁷²³ Alunge, R., *supra* note 686, "The Effect of Africa's Adoption of the EU Notion of Personal Data: The Case of Examination Results" (2019), IST-Africa Conf Proc, at 1-13.

⁷²⁴ Mannion, C., *supra* note 692, "Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets" (2020) 53 *Vanderbilt Journal of Transnational Law* 685-710.

⁷²⁵ Megan Vis-Dunbar, James Williams & Jens H Weber Jahnke, *Indigenous and Community-based Notions of Privacy* (2011) UVic/IPIRG-2011-TR-04, University of Victoria, online:

https://www.researchgate.net/publication/310482039_Indigenous_and_Community-based_Notions_of_Privacy, accessed September 10, 2024

⁷²⁶ *Ibid.*

The GDPR approach focuses heavily on informational privacy by only considering personal data and ignoring non-personal data, a perspective rooted in Eurocentric individualism.⁷²⁷ This contrasts sharply with the communal orientation prevalent in African societies.⁷²⁸ This highlights the necessity of developing privacy and data protection frameworks that align with African cultural norms and values. By respecting and integrating the unique cultural, social, and economic factors across African communities, a culturally attuned approach can effectively address the challenges of adapting Western data privacy norms to African realities.⁷²⁹ The EU framework's emphasis on individualistic protections often diverges from the socio-cultural realities of African countries, where integrated cultural and collective aspects are more prevalent. As outlined in Chapter 3, this disparity presents significant challenges when implementing the EU's privacy and data protection model in Africa. Moreover, initiatives by the AU and RECs, which tend to align with the EU model, further exacerbate these implementation issues.

Given this backdrop, the EU's broad and individualistic conceptualization of personal data necessitates a critical re-evaluation when applied to the African context. For example, the GDPR defines personal data to include a wide spectrum, from names to sensitive physical and psychological data, aiming to support a data-intensive economy.⁷³⁰ However, this extensive scope often clashes with the cultural subtleties and societal structures in Africa, where privacy norms are deeply rooted in communal values and relationships.⁷³¹ In many African societies, personal data is not just an individual asset but is intrinsically linked to communal identities and shared responsibilities,⁷³² thus requiring a more nuanced approach

⁷²⁷ GDPR Art. 4, “Definitions”, Regulation (EU) 2016/679.

⁷²⁸ Owoniyi, S., *supra* note 704, “African Cultural Values: The Past, Present and Future”, at 1–23.

⁷²⁹ *Ibid.*

⁷³⁰ Regulation (EU) 2016/679, *supra* note 53, 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), OJ L 119, 4 May 2016, p. 1.

⁷³¹ Sudarkasa, Niara. “African and Afro-American Family Structure: A Comparison.” *Black Scholar* 11 (November/December 1980): 44. Cited in Cobbah, *supra* note 2.

⁷³² *Ibid.*

that the EU model fails to accommodate. Consequently, in the African context, personal data should be conceptualized from a communal rather than an individualistic perspective.⁷³³ This broader definition would not only cater to individual privacy but also consider the impact of data collection, use, and sharing on the broader community. Data concerning communal lands, local traditions, or community health practices, for instance, should be managed in ways that respect communal rights and values. Such an approach would necessitate crafting privacy and data protection regulations that recognize both individual and community rights, thereby balancing the need for privacy with the communal practices that are prevalent in many African societies.

Moreover, the African context introduces a distinct concept of collective ownership, which diverges from European norms where the framework of privacy and data protection does not typically encompass data ownership.⁷³⁴ In many African societies, privacy and data protection encapsulate both individual and communal interests, reflecting a nuanced interplay rather than a strict dichotomy. Collective ownership is deeply rooted in notions of belonging, responsibility, and communal stewardship, yet it does not exclude the recognition of individual rights.⁷³⁵ Privacy, in this context, is viewed as a shared responsibility that balances the interests of individuals with the well-being of the community, emphasizing relationships, trust, and accountability. While the European model tends to prioritize individual rights, African perspectives on privacy seek to harmonize individual autonomy with the protection of communal assets and social bonds.⁷³⁶ The African cultural anthropology of privacy reveals that it is not a matter of rejecting individual interests but rather one of a degree, where the individual's rights are considered within the broader collective framework. For instance,

⁷³³ Kiggundu, J., *"Giving Teeth to the African Union: Advancing Compliance with Data Privacy Norms"* (2021), 45-65.

⁷³⁴ Naidoo, J., *supra* note 723, "Namibia's Community-Based Natural Resource Management Program: The Politics of Communal Land Tenure and the Management of Local Natural Resources" (2011).

⁷³⁵ *Ibid.*

⁷³⁶ *Ibid.*

decisions regarding the use of communal data or cultural expressions often require collective consent, which inherently includes the voices of individuals as members of the community. African cultural expressions, such as songs, dances, and oral traditions, embody rights and responsibilities that are transmitted through localized cultural processes, representing more than just informational or artistic value.⁷³⁷ These expressions are deeply intertwined with individual and communal identities, making their unauthorized use or dissemination a violation of both personal and collective norms. For example, when technological means are used to capture and distribute these expressions beyond their intended contexts, it disrupts not only communal values but also the rights of individuals who contribute to and are represented by these cultural practices.⁷³⁸ Additionally, African cultural expressions often act as repositories of valuable information, such as clan histories, social relations, and communal rights, which are proprietary to specific families or clans.⁷³⁹ Accessing such stories without permission is akin to breaching both individual and group privacy. This duality highlights the interconnectedness of individual and communal interests within African perspectives on privacy, where safeguarding one often serves to reinforce the other. This mismatch between European and African conceptualizations of privacy and ownership highlights the necessity for regulatory frameworks that are tailored to African traditions and societal structures. Such frameworks must prioritize both individual and collective dimensions of privacy, recognizing that privacy in African contexts is neither purely individualistic nor entirely communal. Instead, it reflects a dynamic balance that aligns with the cultural, social, and economic realities of African communities. By addressing this interplay, regulatory approaches can

⁷³⁷ Onwuekwe, Agatha Ijeoma. "The Socio-Cultural Implications of African Music and Dance" (2012) *Journal of African Music and Dance*, 1-23.

⁷³⁸ Vis-Dunbar, M., Williams, J. & Weber Jahnke, J., *Indigenous and Community-based Notions of Privacy* (2011) UVic/IPIRG-2011-TR-04, University of Victoria, online: https://www.researchgate.net/publication/310482039_Indigenous_and_Community-based_Notions_of_Privacy, accessed September 10, 2024.

⁷³⁹ Onwuekwe, A. I., *supra* note 739, "The Socio-Cultural Implications of African Music and Dance" (2012) *Journal of African Music and Dance*, at 1-23.

resonate more deeply with African societies while safeguarding both individual rights and collective heritage.

Expanding on this analysis, generic global approaches to privacy and data protection often fail to accommodate the unique cultural dynamics prevalent in African societies.⁷⁴⁰ Predominantly Western frameworks prioritize individual privacy and data protection, neglecting the communal aspects that are integral to African societies.⁷⁴¹ Consequently, these models prove inadequate for addressing the collective dimensions of privacy and data protection required in African contexts.⁷⁴² Recognizing these cultural nuances highlights the necessity of developing a tailored approach to privacy and data protection that respects and integrates the distinct cultural, social, and communal attributes of African countries. It is crucial to note that privacy is not inherently a Western construct; forms of privacy exist in every culture worldwide. The difference among cultures lies not in the presence of privacy needs but in how these needs are met and how privacy is regulated. While some scholars argue that privacy is culturally relative, contingent upon the social, moral, and political values of the people living in a given domain, relatively limited attention has been paid to cross-cultural factors in privacy.⁷⁴³ The few studies that have addressed this topic have been inconclusive about the role of culture in privacy and data protection issues. This necessity highlights the importance of examining the cultural foundations of privacy and data protection, particularly in the context of African societies.

5.2 Cultural Foundations of Privacy and Data Protection

The existing privacy and data protection legal frameworks reveal a significant gap: the absence of African cultural perspectives. This omission is primarily due to the dominance of

⁷⁴⁰ Cobbah, J. A. M., *supra* note 674, “African Values and the Human Rights Debate: An African Perspective” (1987) 9(3) *Human Rights Quarterly* 309–331.

⁷⁴¹ Prinsloo, P. & Kaliisa, R., *supra* note 668, “Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics” (2022) *Brit J Educ Technol* 53: 894-913.

⁷⁴² Owoniyi, S., *supra* note 704, “African Cultural Values: The Past, Present and Future”, at 1–23.

⁷⁴³ Cohen, J.E., *supra* note 682, “What Privacy is For” (2013) 126 *Harv L Rev* 1904.

the Eurocentric GDPR model, which has been widely adopted as a benchmark for privacy and data protection without sufficient consideration for Africa's cultural and societal structures. Consequently, African legal frameworks have often uncritically replicated this model without adapting it to the continent's rich cultural contexts.⁷⁴⁴ This regulatory transplantation reinforces a form of legal dependency, reflecting broader TWAIL critiques of global governance structures that marginalize Global South perspectives in international law. This oversight draws attention to the necessity of moving beyond the GDPR to incorporate and prioritize cultural dimensions, recognizing that culture fundamentally shapes societal functions and profoundly influences all aspects of the human experience.⁷⁴⁵ Rather than adopting external regulatory models wholesale, privacy and data protection frameworks in Africa must be embedded in indigenous knowledge systems and governance traditions. A culturally relevant approach recognizes that privacy is not a fixed, universal concept but is shaped by the social values, communal norms, and governance structures that define African societies. As Edward B. Tylor articulated in 1958, culture comprises a comprehensive suite of elements including knowledge, belief, art, morals, laws, and customs, all of which are acquired by individuals as members of society.⁷⁴⁶ This broad definition emphasizes culture as a repository of societal values and norms that guide human interactions and behaviours. Recognizing these elements is vital for developing privacy and data protection regulations that resonate with the diverse cultural landscapes of African societies. Furthermore, Bronisław Malinowski's depiction of culture as a functional, active, and well-organized unity that evolves in response to human needs and environmental factors highlights the necessity for adaptable privacy and data protection frameworks.⁷⁴⁷ Rigid, one-size-fits-all legal instruments, such as the GDPR, fail to account for the localized governance structures and

⁷⁴⁴ Prinsloo, P. & Kaliisa, R., *supra* note 668, "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

⁷⁴⁵ Owoniyi, S., *supra* note 704, "African Cultural Values: The Past, Present and Future", at 1-23.

⁷⁴⁶ Tylor, E.B., "*Primitive Culture*" (1958), Harper Torchbooks, 1-25.

⁷⁴⁷ Malinowski, B., "*A Scientific Theory of Culture*" (1944), University of North Carolina Press.

social values that influence how privacy is understood and exercised in African contexts. Thus, privacy frameworks must be flexible, culturally embedded, and responsive to the socio-economic conditions that shape African digital ecosystems.

Similarly, within the African context, culture represents a complex and multifaceted framework that permeates all aspects of societal structures and individual experiences.⁷⁴⁸ It encompasses a rich spectrum of both tangible and intangible elements, from aesthetic expressions like art, music, and literature to practical realms such as health, education, and social organization.⁷⁴⁹ Thus, African culture is characterized by enduring features that ensure continuity across generations, alongside a dynamic adaptability that responds to internal changes and external pressures.⁷⁵⁰ Moreover, cultural norms in African societies may be explicitly taught or subconsciously assimilated, shaping a shared social legacy within communities.⁷⁵¹ These norms manifest in both visible and subtle ways, influencing individual and collective behaviours, identities, and societal structures. The dual nature of culture in African contexts, as both stable and evolving, demonstrates its profound impact on daily experiences and broader societal dynamics.⁷⁵² Thus, the appropriate approach for the African context demands a framework that not only acknowledges but actively integrates these cultural realities. This integration is essential for drafting privacy and data protection policies that are not only legally robust but also culturally consonant, ensuring they align with the social and economic realities of the continent. Consequently, this culturally attuned approach highlights the critical need for privacy regulations that reflect and respect the unique cultural, social, and communal attributes of African countries, offering a more sustainable and effective model for privacy and data protection.

⁷⁴⁸ Prinsloo, P. & Kaliisa, R., *supra* note 668, “Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics” (2022) *Brit J Educ Technol* 53: 894-913.

⁷⁴⁹ *Ibid.*

⁷⁵⁰ Naidoo, J., *supra* note 723, “Namibia's Community-Based Natural Resource Management Program: The Politics of Communal Land Tenure and the Management of Local Natural Resources” (2011).

⁷⁵¹ *Ibid.*

⁷⁵² Owoniyi, S., *supra* note 704, “African Cultural Values: The Past, Present and Future”, at 1–23.

5.2.1 Balancing Individual and Communal Interests in African Privacy and Data Protection Frameworks.

Privacy and data protection in Africa are deeply influenced by communal governance structures, necessitating frameworks that integrate collective responsibilities while safeguarding individual autonomy.⁷⁵³ This cultural context, which emphasizes community cohesion over individualism, necessitates the development of a bespoke privacy and data protection framework that respects and integrates these fundamental societal principles. While this approach diverges from the predominantly individualistic orientation of European frameworks such as the GDPR, it does not marginalize individual interests. Instead, it seeks to harmonize them with collective responsibilities, reflecting a nuanced interplay between personal autonomy and communal well-being. In this context, privacy and data protection in African societies is conceptualized as a shared responsibility, where safeguarding individual rights inherently reinforces the collective good. For instance, data governance mechanisms involving communal lands or cultural traditions inherently protect the rights of individuals within these communities, thereby ensuring that privacy frameworks remain inclusive and balanced. Balancing individual and communal interests in the African context necessitates a multi-faceted and participatory approach. First, it requires the active engagement of diverse stakeholders, including individuals, community leaders, and policymakers, in the formulation of privacy frameworks. Such inclusive engagement ensures that individual concerns are not subsumed under collective priorities but are addressed within a broader communal context, thereby fostering trust and inclusivity. Second, community-driven governance mechanisms must be established to respect both individual autonomy and collective ownership. For example, the creation of data stewardship councils can provide a platform for mediating

⁷⁵³ Vis-Dunbar, M., Williams, J. & Weber Jahnke, J., *supra* note 740, *Indigenous and Community-based Notions of Privacy* (2011) UVic/IPIRG-2011-TR-04, University of Victoria, online: https://www.researchgate.net/publication/310482039_Indigenous_and_Community-based_Notions_of_Privacy, accessed September 10, 2024.

potential conflicts between individual rights and collective interests, ensuring equitable representation of all stakeholders.

Furthermore, the development of privacy frameworks tailored to the cultural, social, and economic specificities of African communities is essential. Context-sensitive regulations should incorporate mechanisms for collective decision-making, such as requiring community consent for the utilization of shared resources or cultural data. In addition, policymakers and data handlers must undergo cultural sensitivity training to enhance their understanding of the interplay between individual and collective dimensions of privacy. This ensures that privacy policies are not inadvertently skewed towards one dimension at the expense of the other. Technological innovations also hold significant potential in this regard. Digital platforms, for instance, can enable individuals to exercise autonomy through consent mechanisms that align with the collective values of their communities, thereby preserving cultural norms while safeguarding individual rights. By integrating these strategies, privacy frameworks in Africa can effectively balance individual and communal interests, ensuring that both dimensions are equally respected and protected.

Moreover, the African perspective introduces a unique notion of collective ownership that contrasts with European legal frameworks, which are predominantly focused on individual rights to privacy and data protection.⁷⁵⁴ In the African context, ownership extends beyond the individual to encompass communal stewardship, intricately tied to ideas of belonging, responsibility, and shared social obligations. This perspective challenges the adequacy of European legal models, such as the GDPR, in African settings, particularly when it comes to the protection of communal assets and the intricate social bonds that are integral to African communities. Additionally, cultural expressions such as songs and dances, which carry

⁷⁵⁴ Owoniyi, S., *supra* note 704, “African Cultural Values: The Past, Present and Future”, at 1–23.

significant communal value and rights, transcend mere data.⁷⁵⁵ They embody rich historical and social significance that must be protected against unauthorized use and dissemination under the privacy and data protection regime. It becomes apparent that generic global approaches to privacy and data protection often fail to account for the unique cultural dynamics of African societies. Given the communal nature of African societies, privacy frameworks must move beyond Western individualistic models to embrace indigenous governance traditions. Ultimately, this gap illustrates the necessity of developing a tailored approach that respects and integrates the distinct cultural, social, and communal attributes of African countries. Recognizing that privacy is not inherently a Western construct but exists universally across cultures, it is essential to adopt privacy frameworks that reflect the specific social, moral, and political values of African societies.⁷⁵⁶ This tailored approach would ensure that privacy and data protection regulations are culturally resonant and legally effective, catering to the unique needs and conditions of the continent.

In this context, the rich cultural structure of African societies, underpinned by a profound emphasis on community-centric values and collective identity, significantly shapes the conceptualization and enactment of privacy and data protection. Moreover, moving beyond a broad understanding of cultural influences, a closer examination of the specific societal structures in Africa reveals a deep-rooted belief in communal governance and collective identity, where the collective takes precedence over the individual.⁷⁵⁷ Thus, this community-focused worldview paves the way for understanding how African communities uniquely interpret and practice the concepts of self-determination and sovereignty.

⁷⁵⁵ Vis-Dunbar, M., Williams, J. & Weber Jahnke, J., *supra* note 740, *Indigenous and Community-based Notions of Privacy* (2011) UVic/IPIRG-2011-TR-04, University of Victoria, online: https://www.researchgate.net/publication/310482039_Indigenous_and_Community-based_Notions_of_Privacy, accessed September 10, 2024.

⁷⁵⁶ Alunge, R., *supra* note 686, “The Effect of Africa’s Adoption of the EU Notion of Personal Data: The Case of Examination Results” (2019), IST-Africa Conf Proc, at 1-13.

⁷⁵⁷ Prinsloo, P. & Kaliisa, R., *supra* note 668, “Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics” (2022) *Brit J Educ Technol* 53: 894-913.

Importantly, these countries are not merely abstract ideals but are essential in shaping practical approaches to privacy and data protection. As such, as African countries navigate the challenges of modern governance and global interactions, they draw upon their cultural heritage to uphold community-focused values. Therefore, this blend of traditional practices and contemporary needs offers a distinct perspective on privacy and data protection, emphasizing the primacy of the collective alongside the individual.

Taking this into account, the principle of self-determination, grounded in the historical struggles of postcolonial nations, grants countries and societies the right to govern themselves, where the ability to determine their affairs is a key aspect of sovereignty.⁷⁵⁸ While international law recognizes sovereignty as the defining characteristic of statehood, this notion is often undermined by the enduring legacies of colonial legal structures and global power asymmetries. Regulatory frameworks imposed by the Global North tend to reinforce these hierarchies, limiting the ability of African nations to develop independent privacy and data protection laws.⁷⁵⁹ Thus, self-determination and sovereignty serve as crucial foundations for the community-centric privacy frameworks emerging in the African context. These principles challenge the dominant Western liberal model, which prioritizes individualism, and instead advocate for a privacy governance approach that aligns with Africa's collective traditions.⁷⁶⁰

Following this line of thought, the right to self-determination encompasses both individual and collective dimensions, extending beyond the personal to include the communal. As the United Nations Charter articulates, this right is fundamental to communities' social and economic well-being, intrinsically linking their autonomy to their

⁷⁵⁸ Chidi Oguamanam, "Indigenous Peoples, Data Sovereignty, and Self-Determination: Current Realities and Imperatives" (2020) 26 *African Journal of Information and Communication* 1-20.

⁷⁵⁹ Navid Pourmokhtari, "A Postcolonial Critique of State Sovereignty in IR: The Contradictory Legacy of a 'West-centric' Discipline" (2013) 34:10 *Third World Quarterly* 1767-1793.

⁷⁶⁰ Ibid.

ability to manage and safeguard communal data and privacy.⁷⁶¹ This interconnectedness emphasizes the collective nature of self-determination, which is indispensable for fostering community prosperity, identity, and security. In addition to the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP),⁷⁶² which primarily addresses the rights of Indigenous Peoples, self-determination is recognized as a fundamental principle in international law, enshrined in foundational instruments such as the International Covenant on Civil and Political Rights (ICCPR)⁷⁶³ and the International Covenant on Economic, Social and Cultural Rights (ICESCR).⁷⁶⁴ Article 1 of both Covenants affirms that all peoples have the right to self-determination, allowing them to freely determine their political status and pursue their economic, social, and cultural development. This broader foundation highlights that self-determination is a universal right, applicable to all peoples. In the African setting, the principle of self-determination holds particular resonance, given the continent's colonial history and the struggles for liberation and autonomy. African jurisprudence, as reflected in the ACHPR,⁷⁶⁵ advances a distinctive perspective on self-determination. Article 20 of the ACHPR explicitly recognizes the inalienable right of all peoples to self-determination, linking it to their sovereignty over natural resources and the preservation of their cultural heritage. This provision further emphasizes that the collective autonomy of communities is essential for safeguarding their identity and securing their socio-economic and cultural development.

Consequently, privacy and data protection frameworks must be tailored to reflect the specific cultural, social, and economic contexts of African communities. Recognizing this, it

⁷⁶¹ Charter of the United Nations, 26 June 1945, 1 UNTS XVI (entered into force 24 October 1945).

⁷⁶² United Nations Declaration on the Rights of Indigenous Peoples, GA Res 61/295, UN GAOR, 61st Sess, Supp No 49, UN Doc A/RES/61/295 (2007) [adopted 13 September 2007].

⁷⁶³ International Covenant on Civil and Political Rights, GA Res 2200A (XXI), UN GAOR, 21st Sess, Supp No 16, UN Doc A/6316 (1966), 999 UNTS 171 (entered into force 23 March 1976).

⁷⁶⁴ International Covenant on Economic, Social and Cultural Rights, GA Res 2200A (XXI), UN GAOR, 21st Sess, Supp No 16, UN Doc A/6316 (1966), 993 UNTS 3 (entered into force 3 January 1976).

⁷⁶⁵ African Charter on Human and Peoples' Rights, 27 June 1981, OAU Doc CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982) (entered into force 21 October 1986).

becomes imperative to understand that while the terms ‘sovereignty’ and ‘self-determination’ are often used interchangeably, self-government forms a distinct and critical component of sovereignty. Self-government is pivotal in maintaining the social organization of African communities, encompassing a range of powers and responsibilities vital for the preservation and enhancement of community identity and social structures. This includes legislative authority, which enables communities to establish privacy and data protection frameworks that resonate with their unique socio-cultural contexts. By embedding these principles into privacy and data protection frameworks, for instance, through participatory law-making processes, community-based data governance models, and recognition of customary norms in legislative design, African societies can ensure that these measures not only protect individual and communal autonomy but also reflect the intrinsic values and aspirations of their communities. This ensures that privacy and data protection frameworks align with the broader jurisprudential understanding of self-determination as a universal principle that transcends specific contexts, addressing the unique challenges and opportunities within the African environment.

5.2.2 Community-Centric Privacy and Data Protection: Lessons from Indigenous Practices

Given the deep-rooted influence of cultural dimensions in African societies, it is essential to examine how indigenous governance structures can inform privacy and data protection frameworks. African societies, characterized by complex communal governance and collective identity, present a distinct contrast to Western models that emphasize individualistic legal principles. This divergence highlights the necessity of community-centric approaches to privacy and data protection, particularly in the context of evolving digital technologies. By learning from indigenous traditions that uphold communal rights and shared

responsibilities, privacy regulations in Africa can better reflect societal values and governance systems.

The incorporation of community-centric practices into privacy regulation aligns with a decolonial theoretical framework that challenges the Eurocentrism embedded in global legal norms.⁷⁶⁶ The dominance of Western individualistic norms in privacy and data protection regulations often fails to account for the unique cultural, social, and economic contexts of African societies. By centering the perspectives and practices of African communities, a more context-sensitive and culturally relevant understanding of privacy and data protection can emerge. For instance, across African communities, decision-making processes concerning communal data, such as information about ethnic groups or lands, are inherently shaped by the norms and traditions of the communities themselves rather than external interventions.⁷⁶⁷ This ensures that external interventions, where present, must align with pre-existing community norms rather than redefine them. Consultation and consensus within the group drive decision-making, emphasizing the self-determined and collective nature of African approaches. This collaborative approach differs fundamentally from Western practices that prioritize individual consent, reflecting a more holistic and community-oriented approach to privacy and data protection.

Similarly, the Maasai communities in Kenya and Tanzania illustrate a community-driven approach to governance. Specifically, leaders convene meetings with all community members to collectively address issues impacting the entire group, such as the management of communal lands.⁷⁶⁸ The Maasai Wilderness Conservation Trust (MWCT) in Kenya exemplifies this model of community-driven governance, where the Maasai's pre-existing

⁷⁶⁶ Ibid.

⁷⁶⁷ Cath Traynor et al., *Community Protocols in Africa: Lessons Learned for ABS Implementation* (2018) Natural Justice.

⁷⁶⁸ Unks, R. R. et al., "Diffuse Land Control, Shifting Pastoralist Institutions, and Processes of Accumulation in Southern Kenya" (2023) 50(5) *The Journal of Peasant Studies* 1757-1790, and Ameso, E. A. et al., "Pastoral Resilience among the Maasai Pastoralists of Laikipia County, Kenya" (2018) 7(2) *Land* 78.

norms of stewardship shape the external interventions.⁷⁶⁹ These norms dictate collaboration with conservation professionals, including partners like US Board President Edward Norton, to protect East Africa's ecosystems while ensuring direct benefits to the Maasai people.⁷⁷⁰ MWCT's programs focus on the Chyulu Hills, a crucial part of the Amboseli-Tsavo Ecosystem that provides water to millions in Kenya. Their efforts promote sustainable economic benefits from conservation, establishing a model for community stewardship that integrates external expertise while maintaining community-driven priorities. Similarly, the traditional chieftaincy system in Ghana plays a crucial role in collective governance. Chiefs, elected based on lineage and communal consensus, oversee community gatherings and manage traditional lands and customs, even in modern urban settings.⁷⁷¹ This facilitates communal decision-making that respects collective privacy and heritage.

Although these examples do not pertain specifically to privacy and data protection, they highlight the importance of integrating community-centric practices into data protection frameworks. By doing so, policymakers can ensure that privacy and data protection regulations are not only legally robust but also culturally consonant, aligning with the social and economic realities of the continent. Rather than transplanting foreign models, Africa must cultivate regulatory frameworks that respect indigenous decision-making structures while safeguarding individual and collective privacy rights. By integrating these strategies, privacy frameworks can better serve African communities, ensuring that both personal autonomy and communal governance are harmonized within data protection policies.

5.2.3 Collective Approach

⁷⁶⁹ Maasai Wilderness Conservation Trust, *Equator Initiative Case Study* (2013) UNDP, and United Nations Development Programme, *Maasai Wilderness Conservation Trust, Kenya* (2013), Equator Initiative Case Study Series.

⁷⁷⁰ Ibid.

⁷⁷¹ Emmanuel Debrah, "Participation of Chiefs in Decentralised Local Governance in Ghana" (2022) 26 *Commonwealth Journal of Local Governance* 53-73.

In the contemporary discourse on privacy and data protection, there is a compelling need to consider frameworks that resonate with the unique cultural contexts of different societies. For African communities, the concept of privacy cannot be adequately addressed through the individualistic paradigms that dominate Western legal frameworks. Instead, a collective approach to privacy and data protection, which emphasizes the autonomy and integrity of the community, offers a more culturally congruent model.⁷⁷² This approach not only reflects the deeply rooted communal values and collective identities in African societies but also provides a well-grounded framework for addressing privacy and data protection in ways that are both effective and respectful of local contexts.⁷⁷³ The collective approach amplifies the community's rights to self-governance and control over its information, aligning with traditional values of communal decision-making and self-determination.⁷⁷⁴ By recognizing the community as a central entity in privacy and data protection, this approach ensures that privacy regulations resonate with the social and cultural values of African societies. It emphasizes the community's collective rights to manage and protect its information, ensuring that privacy regulations are not only relevant but also sustainable.⁷⁷⁵

Furthermore, the collective approach supports individual privacy while also reflecting broader communal relationships, responsibilities, and objectives.⁷⁷⁶ This conceptualization of privacy and data protection aligns with traditional African values, where the community's well-being is paramount, and decisions are made collectively to ensure the interests of all members are considered. By adopting a collective approach to privacy and data protection, policymakers can create frameworks that are more attuned to the cultural, social, and

⁷⁷² Vis-Dunbar, M., Williams, J. & Weber Jahnke, J., *supra* note 740, *Indigenous and Community-based Notions of Privacy* (2011) UVic/IPIRG-2011-TR-04, University of Victoria, online: https://www.researchgate.net/publication/310482039_Indigenous_and_Community-based_Notions_of_Privacy, accessed September 10, 2024.

⁷⁷³ *Ibid.*

⁷⁷⁴ *Ibid.*; Prinsloo, P. & Kaliisa, R., *supra* note 668, "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

⁷⁷⁵ Cobbah, J. A. M., *supra* note 674, "African Values and the Human Rights Debate: An African Perspective" (1987) 9(3) *Human Rights Quarterly* 309-331.

⁷⁷⁶ *Ibid.*

economic realities of African communities. This shift from an individualistic to a collective perspective in privacy and data protection governance not only enhances the effectiveness of privacy and data protection regulations but also ensures they are culturally relevant and respectful of African communal values. Thus, the collective approach presents a viable and necessary alternative to the predominant Western models, addressing the unique needs and contexts of African societies. The longstanding recognition of communal values in managing private and public life underlines that although privacy is often viewed as a modern concern, many cultures, including those in Africa, have deep-rooted norms that dictate the balance between private and public life, specifying appropriate times and manners for their intersection.⁷⁷⁷

Similarly, the collective approach to privacy and data protection involves collective ownership, which is integral to African societies.⁷⁷⁸ In these communities, collective rights over shared knowledge and cultural practices are as significant as individual rights over personal information.⁷⁷⁹ Consequently, this approach empowers communities to control access to and usage of information derived from their cultural heritage. This framework emphasizes that individual privacy is inherently linked to collective well-being, highlighting the interconnected nature of individual and communal interests in African contexts.⁷⁸⁰ Extending beyond the protection of personal data, this approach incorporates non-personal data, recognizing their importance in maintaining cultural integrity. African privacy norms prioritize sustaining cultural heritage and fostering relationships characterized by belonging, responsibility, and respect.⁷⁸¹ This relational approach necessitates privacy frameworks that

⁷⁷⁷ Owoniyi, S., *supra* note 704, “African Cultural Values: The Past, Present and Future”, at 1–23.

⁷⁷⁸ Lukman Abdulrauf, “African Approach(es) to Data Protection Law” (2024) in *Data Protection Law in Africa*, De Gruyter, 31-53.

⁷⁷⁹ Naidoo, J., *supra* note 669, “Namibia's Community-Based Natural Resource Management Program: The Politics of Communal Land Tenure and the Management of Local Natural Resources” (2011).

⁷⁸⁰ Prinsloo, P. & Kaliisa, R., *supra* note 668, “Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics” (2022) *Brit J Educ Technol* 53: 894-913.

⁷⁸¹ Cobbah, J. A. M., *supra* note 674, “African Values and the Human Rights Debate: An African Perspective” (1987) 9(3) *Human Rights Quarterly* 309–331.

honour the communal essence of African societies, ensuring that both individual rights and collective integrity are safeguarded. The emphasis on communal values challenges dominant Eurocentric models, which often fail to account for these critical aspects of African socio-cultural dynamics. By prioritizing a collective approach, privacy and data protection frameworks can be more culturally relevant and effective, reflecting the social structures and values that underpin African communities.

Integrating collective privacy norms into African societies, rooted in customary laws and communal governance, provides a robust foundation for understanding and managing data sovereignty. These communal approaches to privacy, which emphasize belonging, responsibility, and respect, offer a culturally resonant framework for privacy and data protection governance.⁷⁸² By adopting these approaches, privacy regulations can better reflect the socio-cultural environment of African communities, thereby challenging the conventional individual-centric data protection models. Traditional African practices of ownership, control, access, and possession present a viable alternative to Western data protection models. These practices align privacy and data protection with communal norms, resulting in more effective and culturally appropriate frameworks.⁷⁸³ Such alignment is crucial for addressing the unique privacy and data protection challenges faced by African societies. Embracing these traditional norms allows policymakers to develop strategies that are not only legally effective but also culturally sensitive and sustainable. This approach ensures that privacy regulations respect and integrate the collective dimensions of African cultural heritage, making them both effective and relevant to the local context. Consequently, this perspective promotes a privacy and data protection model that truly resonates with the lived experiences and values of African communities.

⁷⁸²Abdulrauf, L., supra note 780, “African Approach(es) to Data Protection Law” (2024) in *Data Protection Law in Africa*, De Gruyter, at 31-53.

⁷⁸³ Ibid.

5.2.4 Integrating African Cultural Perspectives into Privacy and Data Protection Frameworks

The cultural views on privacy and data protection between Europe and Africa differ significantly, particularly in the emphasis placed on the individual versus the collective.⁷⁸⁴ African societies have traditionally prioritized the community, focusing on collective identity and agency rather than individualism.⁷⁸⁵ Historically, individuals were primarily regarded as integral parts of larger community collectives, with a focus on promoting group interests over personal gains. As these traditional perspectives adapt to the digital era, they have evolved into more complex and nuanced understandings of rights and responsibilities, especially in the context of digital privacy and data protection.⁷⁸⁶ Within African cultures, rights and obligations are comprehended through a relational framework shaped by communal values.⁷⁸⁷ This perspective perceives the group as a cohesive entity, akin to a living system where each member contributes to the overall well-being of the collective.⁷⁸⁸ Acts of loyalty, generosity, and fulfilling communal responsibilities are viewed as extensions of self-care.⁷⁸⁹ These cultural norms have historically ensured the protection of both individuals and the collective, analogous to modern privacy and data protection concepts, as discussed in the thesis.

African cultural practices assert that individuals, defined by their kinship ties, shared interests, and social standing, are intrinsically connected as components of a larger collective.⁷⁹⁰ This relational perspective, deeply embedded in African societies, informs the understanding of rights and responsibilities, thereby shaping approaches to privacy and data protection. Adherence to African customs necessitates the recognition and protection of both

⁷⁸⁴ Cobbah, J. A. M., *supra* note 674, “African Values and the Human Rights Debate: An African Perspective” (1987) 9(3) *Human Rights Quarterly* 309–331.

⁷⁸⁵ Owoniyi, S., *supra* note 704, “African Cultural Values: The Past, Present and Future”, at 1–23.

⁷⁸⁶ Abdulrauf, L., *supra* note 780, “African Approach(es) to Data Protection Law” (2024) in *Data Protection Law in Africa*, De Gruyter, at 31–53.

⁷⁸⁷ Owoniyi, S., *supra* note 704, “African Cultural Values: The Past, Present and Future”, at 1–23.

⁷⁸⁸ *Ibid.*

⁷⁸⁹ *Ibid.*

⁷⁹⁰ *Ibid.*

collective and individual privacy rights, as well as an appreciation of the significance of non-personal data within privacy and data protection frameworks.⁷⁹¹ This conceptualization marks a critical departure from the predominantly individualistic models that underpin Eurocentric legal systems, as elaborated in this thesis. Central to this African perspective is the role of custodians, who are often entrusted with the management and control of cultural knowledge vital for the survival and identity of the community.⁷⁹² Chiefs and cultural leaders, for example, safeguard the dissemination of such knowledge, ensuring it is shared in ways that align with community norms and respect its sacred value.⁷⁹³ Similarly, sacred sites and locations of cultural significance fall under the stewardship of these leaders, emphasizing the spatial dimension of privacy in African traditions. This highlights the integral connection between privacy, cultural heritage, and place within the African context.

Bridging these traditional practices with contemporary demands requires integrating African privacy norms into modern privacy and data protection frameworks. This integration necessitates a context-sensitive understanding of the unique cultural, social, and economic contexts of African communities. Such an approach not only preserves the integrity and continuity of African cultural heritage but also promotes self-determination and autonomy in the digital age. By embedding culturally rooted perspectives into privacy and data protection policies, policymakers can craft frameworks that are both effective and respectful of the socio-cultural dynamics of African societies. This inclusive and context-sensitive approach fosters a more equitable and sustainable framework for privacy and data protection governance. A key component of this integration involves recognizing the historical influences that have shaped current legal frameworks, particularly the enduring impact of colonialism on African customary law and privacy governance. Colonial legal systems

⁷⁹¹ Ibid.

⁷⁹² Prinsloo, P. & Kaliisa, R., *supra* note 668, “Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics” (2022) *Brit J Educ Technol* 53: 894-913.

⁷⁹³ Owoniyi, S., *supra* note 704, “African Cultural Values: The Past, Present and Future”, at 1–23.

imposed Western legal principles that often disregarded indigenous privacy norms, leading to the marginalization of traditional governance structures in contemporary regulatory frameworks. Revisiting and reintegrating African privacy norms within legal frameworks is therefore a crucial step toward decolonizing data protection laws and ensuring that African societies maintain sovereignty over their digital and informational landscapes. By fostering a legal environment that respects indigenous privacy traditions while accommodating modern technological realities, African states can develop privacy frameworks that are both effective and culturally resonant. This inclusive and context-sensitive approach not only preserves the integrity of African cultural heritage but also promotes regulatory independence, ensuring that data protection laws are designed to serve African communities rather than merely mirroring external legal models.

5.3 A New Paradigm for Privacy and Data Protection in Africa

5.3.1 Ownership in Social Contexts: Individual and Collective Perspectives

To develop a privacy and data protection framework that is contextually appropriate for Africa, the principle of ownership must be central to the discourse. Historically, ownership has been a foundational element in African societies, influencing social relationships and delineating the rights of individuals and communities over property.⁷⁹⁴ This concept is deeply embedded in cultural contexts, similar to the Roman notion of absolute ownership, which conferred unrestricted rights to use, control, and dispose of property.⁷⁹⁵ However, over time, the concept of ownership has evolved, and contemporary legal frameworks now recognize ownership as a bundle of rights, including rights of use, disposition, and duration, tempered by social and legal norms.⁷⁹⁶ In African societies,

⁷⁹⁴ Cobbah, J. A. M., “African Values and the Human Rights Debate: An African Perspective” (1987) 9(3) *Human Rights Quarterly* 309–331.

⁷⁹⁵ Prinsloo, P. & Kaliisa, R., *supra* note 668, “Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics” (2022) *Brit J Educ Technol* 53: 894-913.

⁷⁹⁶ Mamdani, M., *Define and Rule: Native as Political Identity* (2012), Harvard University Press.

however, ownership extends beyond the individualistic paradigm and incorporates significant collective dimensions.⁷⁹⁷ Many indigenous African cultures emphasize communal ownership, where land, resources, and property are held by families or communities, various socio-cultural institutions and entities rather than by individuals. This communal approach reflects broader cultural values that prioritize collective well-being over individual possession.⁷⁹⁸ Accordingly, ownership in African contexts is not limited to mere possession but includes broader rights, such as the ability to occupy, use, profit from, sell, or exclude others from the property.

Beyond models such as the Maasai's communal land tenure system,⁷⁹⁹ other African collective ownership models can inform the development of privacy and data protection frameworks. In South Africa, the concept of *ubuntu*, which emphasizes communalism and interconnectedness, has shaped local approaches to governance and resource management.⁸⁰⁰ This concept could be extended to digital data governance, where data is treated as a collective asset that benefits all community members. These examples demonstrate that African communities already have governance structures that prioritize collective well-being, and these structures can be adapted for digital privacy frameworks. For instance, data could be governed through locally established Data Stewardship Councils that include traditional leaders, community elders, and civil society representatives. These councils would oversee how data is collected, stored, and used, ensuring alignment with both community values and individual privacy rights.

⁷⁹⁷ Ibid.

⁷⁹⁸ Owoniyi, S., "African Cultural Values: The Past, Present and Future", at 1–23.

⁷⁹⁹ Unks, R. R. et al., "Diffuse Land Control, Shifting Pastoralist Institutions, and Processes of Accumulation in Southern Kenya" (2023) 50(5) *The Journal of Peasant Studies* 1757-1790, and Ameso, E. A. et al., supra note 117, "Pastoral Resilience among the Maasai Pastoralists of Laikipia County, Kenya" (2018) 7(2) *Land* 78.

⁸⁰⁰ In African scholarship, Ubuntu is understood as an African philosophy emphasizing collectivist human relationships and assistance in everyday life, whereby individuals are subject to communal considerations. While primarily developed in South African scholarship, the concept also resonates in other African societies.

One potential area of tension in the African context is the intersection between individual privacy rights and communal responsibilities.⁸⁰¹ For instance, in rural communities where land and resources are collectively owned, data concerning communal land use or health information may be perceived as a shared asset. This communal understanding can conflict with individual privacy rights when individuals seek to assert control over information that the community views as collectively held. To balance these competing interests, privacy frameworks in Africa must explicitly recognize the dual nature of data ownership, acknowledging both individual rights and collective ownership in matters of communal significance. Data Stewardship Councils, as previously proposed, could serve as critical mediating bodies in resolving such conflicts. These councils would ensure that communal data is managed in a manner that respects both the individual's privacy rights and the community's collective interests. Furthermore, they could serve as decision-making bodies for disputes related to data governance, ensuring that privacy frameworks remain flexible, contextually adapted, and culturally relevant. They would also facilitate consent processes for the use of shared data, protect against data misuse by third parties, and help ensure equitable benefit-sharing when data generates value, such as in research or commercial contexts.

Given the centrality of communal ownership in African societies, policymakers must translate these cultural principles into data protection frameworks. A framework that neglects collective ownership risks not only being ineffective but also alienating the communities it aims to serve. To operationalize collective ownership within data protection, a multifaceted approach is necessary, incorporating community consultation, stewardship bodies, ethical standards, and collective legal rights. First, community consultation should be integral to the legislative process. Legislators must engage directly with local communities to ensure that

⁸⁰¹ Prinsloo, P. & Kaliisa, R., "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

the voices of traditional leaders, elders, and other stakeholders shape privacy and data protection laws. This approach ensures that governance frameworks are consistent with both individual and collective rights while being attuned to local practices and values. Second, the establishment of Data Stewardship Councils at both national and local levels would provide an essential mechanism for bridging traditional leadership structures with modern regulatory frameworks. These councils, composed of community representatives, could act as intermediaries, ensuring that data collection and usage practices align with local norms, and that benefits derived from data use are equitably distributed within communities. Such councils would also ensure that data protection is not a top-down regulatory exercise but engages communities as active participants in data governance. Third, it is essential to enforce ethical obligations regarding the use of communal data. Laws must include provisions for auditing organizations and governments to ensure they fulfill their responsibilities as data stewards. These obligations should be clearly defined in legal texts, explicitly outlining the duties of data handlers to respect and protect the collective ownership of data. This would involve both safeguarding data integrity and ensuring their ethical use by communal expectations and rights. Finally, the legal framework should provide pathways for communities to assert their collective rights. This requires mechanisms that allow not only individuals but also communities to bring legal challenges when collective data rights are violated. For instance, if data concerning communal resources, cultural heritage, or public health is misused, communities should have the ability to seek redress. Strengthening the legal standing of communities in this regard is crucial to ensuring that privacy and data protection laws are responsive to the collective dimensions of ownership in African societies.

Through these combined measures, African countries can create a privacy and data protection framework that truly reflects their socio-cultural and legal contexts, ensuring that data governance respects the principle of collective ownership while fostering equitable and

culturally relevant legal standards. Furthermore, ownership can be understood as a social arrangement where individuals respect the property rights of others, refraining from taking or using what belongs to someone else. In this relationship, ownership includes the rights to occupy, use, profit from, sell, and exclude others from the property.⁸⁰² Collective psychological ownership can also emerge, where a group collectively feels a sense of ownership over shared resources or territories.⁸⁰³ In the legal context, ownership has traditionally been viewed in terms of intellectual property rather than privacy and data protection.⁸⁰⁴ However, extending the concept of ownership to include data is necessary to address the African context effectively. Integrating the concept of data ownership into legislation across Africa is essential for contextualizing privacy and data protection. It is crucial to identify who owns the data and the extent of ownership held by data subjects over personal data or by communities over collective data. While data is not rivalrous like tangible goods, meaning it can be shared without diminishing its form, contextualizing data ownership within privacy and data protection frameworks can enhance these strategies.⁸⁰⁵ By adopting these principles, African countries can promote autonomy, safeguard cultural heritage, and ensure data governance frameworks remain aligned with collective and individual ownership values. Recognizing and integrating African customary laws within these frameworks will foster more culturally resonant and effective approaches to data governance.

5.3.2 Integrating Collective Ownership into Privacy and Data Protection Frameworks

Building upon this foundation, it is essential to explore the concept of collective data ownership within African communities. This principle, which differs markedly from Western

⁸⁰² Janis Wong, Tristan Henderson & Kirstie Ball, “Data Protection for the Common Good: Developing a Framework for a Data Protection-Focused Data Commons” (2022) 4: e3 *Data & Policy*.

⁸⁰³ Maykel Verkuyten & Borja Martinovic, “Collective Psychological Ownership and Intergroup Relations” (2017) 12(6) *Perspectives on Psychological Science* 1021-1039.

⁸⁰⁴ Wong, J., Henderson, T. & Ball, K., “Data Protection for the Common Good: Developing a Framework for a Data Protection-Focused Data Commons” (2022) 4: e3 *Data & Policy*.

⁸⁰⁵ Ibid.

individualistic perspectives, emphasizes the importance of incorporating communal values into privacy and data protection frameworks. By doing so, these frameworks become not only more culturally relevant but also more effective in practice. The principle of collective data ownership in African societies highlights the communal nature of data, often viewed as a resource owned by the community or family rather than by an individual.⁸⁰⁶ This perspective stands in stark contrast to the Western, individualistic notion of data ownership, aligning more closely with the understanding that community data originates from a collective source and should be governed accordingly. A flexible legal system that harmonizes both customary and statutory laws allows for a more culturally attuned and responsive governance model in Africa. The integration of multiple legal traditions, statutory, customary, and indigenous, within privacy and data protection frameworks is essential to ensuring these systems accurately reflect the lived realities of diverse African societies.⁸⁰⁷ This polycentric governance approach, where authority is distributed across various levels from local communities to national governments enables the creation of adaptable privacy frameworks. Such frameworks respect local customs while simultaneously maintaining consistency across the broader legal landscape.

This approach acknowledges the necessity of plural legal systems that cater to the collective values and cultural practices of African communities, moving beyond the one-size-fits-all model often imposed by international legal frameworks. Consequently, the concept of data stewardship becomes increasingly significant. In this context, organizations or individuals responsible for data collection are not merely data collectors or controllers as referred to in Western principles and the GDPR, but rather data stewards who are entrusted with the protection and ethical management of data. This stewardship model reflects the

⁸⁰⁶ Cobbah, J. A. M., “African Values and the Human Rights Debate: An African Perspective” (1987) 9(3) *Human Rights Quarterly* 309–331.

⁸⁰⁷ Alunge, R., “The Effect of Africa’s Adoption of the EU Notion of Personal Data: The Case of Examination Results” (2019), IST-Africa Conf Proc, at 1-13.

unique African value system, emphasizing the responsibility of those handling data to respect and uphold the collective interests of the community from which the data originates.

Given this, the benefits derived from data should be shared with the community, ensuring that data collection and usage respect elements not included in current legal frameworks of privacy and data protection, such as cultural heritage and ancestral knowledge. Applying these principles to privacy and data protection means recognizing that ownership in African contexts involves a social arrangement where individuals refrain from using what belongs to someone else without consent. This aligns with the idea of collective psychological ownership, where groups perceive ownership over shared resources such as land, neighbourhoods, and even data.⁸⁰⁸ Consequently, data protection policies in Africa should prioritize collective benefit, stewardship, and cultural sensitivity. This emphasis is critical because the complexities surrounding data ownership are evident in ongoing legal debates.⁸⁰⁹ Notably, data lacks a clear legal status as property under common or civil law, which complicates issues related to ownership and control.⁸¹⁰ Existing legal frameworks usually address the rights and obligations related to data rather than directly tackling the concept of data ownership.⁸¹¹ Therefore, it is imperative for the African approach, which situates data ownership within its unique context, to explicitly define data ownership and embed this concept into the legal framework. This strategy highlights the importance of focusing on the responsibilities of data subjects, controllers, and processors in managing data ethically and adhering to communal norms.

⁸⁰⁸ Verkuyten, M. & Martinovic, B., "Collective Psychological Ownership and Intergroup Relations" (2017) 12(6) *Perspectives on Psychological Science* 1021-1039.

⁸⁰⁹ British Academy, Royal Society & techUK, *Data Ownership, Rights and Controls: Reaching a Common Understanding* (2018), seminar summary, British Academy, Royal Society, and techUK; Wong, J., Henderson, T. & Ball, K., "Data Protection for the Common Good: Developing a Framework for a Data Protection-Focused Data Commons" (2022) 4: e3 *Data & Policy*.

⁸¹⁰ Ibid.

⁸¹¹ Ibid.

Building on these principles, integrating Indigenous African principles of collective ownership and stewardship into data protection frameworks can enhance privacy strategies by ensuring they are culturally relevant and respectful of community values. By adopting a model that emphasizes collective ownership, stewardship, shared benefit, and respect for cultural heritage, African societies can develop data protection policies that align with their unique cultural, social, and economic realities, promoting community empowerment and self-determination in the digital era. This principle of collective ownership is deeply rooted in many African cultural traditions, manifesting across diverse social, economic, and cultural dimensions.⁸¹² Understanding these traditional practices provides valuable insights into effectively applying the concept of collective ownership to the emerging field of data governance in Africa. For instance, the communal land tenure systems found in African cultures, such as those practiced by the Maasai of East Africa, where communities rather than individuals hold land rights, highlight this approach. The Maasai employ a communal land tenure model where land is collectively managed by the community, allowing for equitable resource distribution and sustainable land use.⁸¹³ Such systems emphasize the role of the community as a steward, which can serve as a model for collective data management, ensuring sustainable and equitable data utilization.

Integrating the concepts of collective data ownership and stewardship into existing legal frameworks, while also preserving communal data and cultural heritage, establishes a strong foundation for rethinking privacy and data protection in ways that align with traditional values and practices. This incorporation of indigenous principles paves the way for culturally resonant and socially equitable frameworks, offering a clear alternative to the individualistic paradigms dominant in Western legal systems. African societies, with their

⁸¹² Owoniyi, S., “African Cultural Values: The Past, Present and Future”, at 1–23.

⁸¹³ Unks, R. R. et al., “Diffuse Land Control, Shifting Pastoralist Institutions, and Processes of Accumulation in Southern Kenya” (2023) 50(5) *The Journal of Peasant Studies* 1757-1790, and Ameso, E. A. et al., “Pastoral Resilience among the Maasai Pastoralists of Laikipia County, Kenya” (2018) 7(2) *Land* 78.

deep-seated traditions of collective ownership and stewardship, provide distinct models that prioritize community well-being and collective responsibility. Aligning privacy and data protection strategies with these indigenous principles not only safeguards individual privacy but also empowers communities, fostering self-determination.

A significant example of communal reconciliation and collective governance is the *Mato Oput* process among the Acholi community in northern Uganda. This traditional conflict resolution mechanism emphasizes communal participation, reconciliation, and restoring social harmony.⁸¹⁴ While the *Mato Oput* process is not directly concerned with privacy or data protection, its principles of collective responsibility, trust-building, and inclusivity offer a conceptual framework that can be adapted to address challenges in privacy and data protection governance. For instance, privacy and data protection frameworks inspired by such principles could incorporate participatory mechanisms that foster reconciliation and accountability in privacy breaches or data misuse. The emphasis on collective ownership and shared responsibility within *Mato Oput* emphasizes the relevance of Indigenous practices in developing culturally contextual approaches to privacy and data protection.

Similarly, Rwanda's traditional *Gacaca* court system,⁸¹⁵ primarily utilized for post-genocide reconciliation, provides a model for integrating community-based approaches into contemporary legal frameworks. The *Gacaca* courts operated on transparency, collective participation, and fairness principles, ensuring that justice processes resonated with communal values and fostered trust. Although not explicitly focused on privacy, these principles can be extrapolated to inform the development of privacy and data protection mechanisms that prioritize community engagement and collective oversight. For example,

⁸¹⁴ Okello Lucima, "Reconciliation and Justice: 'Mato Oput' and the Amnesty Act 2002" (2010), online: Conciliation Resources <https://www.c-r.org/accord/northern-uganda/reconciliation-and-justice-%E2%80%98mato-oput%E2%80%99-and-amnesty-act-2002>, accessed September 1, 2024.

⁸¹⁵ Nyseth Brehm, H., Uggen, C. & Gasanabo, J.-D., "Genocide, Justice, and Rwanda's Gacaca Courts" (2014) 30(3) *Journal of Contemporary Criminal Justice* 333-352.

localized privacy councils or data protection governance committees could draw from the *Gacaca* model, mediating disputes and ensuring equitable data management in ways that respect individual and communal interests. The principles underlying these systems, collective accountability, reconciliation, and shared stewardship, can be reinterpreted and applied to design privacy frameworks that align with the socio-cultural dynamics and values of African communities.

5.3.3 Redefining the Principle of Access in Privacy and Data Protection Frameworks

The right of access to personal data is a cornerstone of privacy and data protection frameworks, enabling individuals to verify the accuracy of their information, correct inaccuracies, and understand how their data is utilized. This right not only empowers data subjects to exercise additional rights, such as rectification and erasure but also fosters transparency and accountability in data management. However, in the African context, characterized by resource constraints and underdeveloped infrastructure, a more innovative and contextually adapted approach is essential for effective implementation. While the GDPR highlights the right of access within a broader framework of data protection rights,⁸¹⁶ imposing strict penalties for non-compliance, the structured and resource-intensive approach of the GDPR may not be transferable to African contexts. The conventional two-stage process, first determining whether personal data related to the individual is being processed and then providing detailed information on the processing,⁸¹⁷ presents significant challenges in environments with limited technological and human resources. To ensure feasibility without compromising rights, the principle of access in African contexts must be adapted to reflect the realities of these constraints. Simplification in this regard does not entail a reduction of rights but rather an adaptation that enables individuals to exercise their rights

⁸¹⁶ General Data Protection Regulation (EU) 2016/679, *Articles 12, 15, and 46*, and *Recitals 58, 63, 64, and 73*.

⁸¹⁷ *Ibid.*

meaningfully within their socio-economic conditions. This could involve the development of community-based data access centers, mobile data request units, or the use of local intermediaries, such as trained village clerks who can assist individuals in submitting access requests and understanding their rights.

In regions with diverse connectivity levels and digital infrastructure, technology solutions must be tailored accordingly. For instance, while mobile technologies such as M-Pesa have proven effective in Kenya,⁸¹⁸ other regions with lower levels of internet access require more adaptive solutions. For populations in remote areas with limited or no internet access, and for individuals who lack access to even basic mobile phones or the literacy to operate them, alternative mechanisms must be developed. Community-based privacy advocates or intermediaries could play a critical role in bridging this gap. These advocates, trained in data protection principles and privacy frameworks, could assist individuals in managing their personal data and understanding their rights. This approach ensures inclusivity for those unable to access or operate digital tools. Additionally, Unstructured Supplementary Service Data (USSD) based technologies,⁸¹⁹ which operate on basic mobile phones, can be utilized for privacy protection and personal data management. These low-tech solutions enable individuals to monitor their data usage and report concerns through simple text-based interfaces. In countries like Uganda and Tanzania, where mobile penetration is high but internet connectivity is limited, similar USSD platforms could be developed to enable individuals to manage consent for data use, offering a straightforward mechanism to ensure privacy protection even without smartphones or high-speed internet.

⁸¹⁸ Isaac Mbiti & David N. Weil, *Mobile Banking: The Impact of M-Pesa in Kenya* (2011) NBER Working Paper No. 17129, National Bureau of Economic Research.

⁸¹⁹ Unstructured Supplementary Service Data (USSD) is a service that allows mobile phone users to interact with a remote application from their device in real time. A predefined session is initiated when a user dials in, enabling the transfer of information between the application and the user. USSD is a highly scalable service, as it does not require an internet connection and is supported by both feature phones and smartphones (see: <https://africastalking.com/ussd>).

Additionally, governments could invest in digital literacy programs targeting rural areas, ensuring citizens understand their rights under new privacy frameworks and can effectively utilize available technology. These programs should be designed in multiple local languages, with culturally and contextually relevant content to the diverse communities across the continent. Nonetheless, it is imperative to recognize that a significant proportion of the African population, including both rural and urban communities, faces substantial barriers to accessing and utilizing digital tools. Many individuals lack access to smartphones, basic mobile phones, or reliable internet connectivity. Even in cases where such technology is available, varying levels of general and digital literacy further hinder their ability to meaningfully engage with privacy frameworks. These challenges demand a multifaceted approach that transcends reliance on digital solutions alone and integrates alternative, inclusive methods of outreach and education. To bridge these gaps, privacy education programs must incorporate offline and in-person mechanisms that cater to the realities of these populations. For example, community-based workshops led by trained facilitators can provide direct engagement on privacy rights and data protection concepts. Additionally, leveraging traditional communication platforms such as local radio stations and printed materials ensures broader accessibility. For populations with limited literacy, innovative approaches such as oral storytelling and participatory discussions can effectively convey complex legal and technical concepts in accessible formats. Such methods must be thoughtfully tailored to align with the cultural and linguistic diversity of African communities, ensuring their relevance and resonance. Moreover, these programs should not only focus on imparting knowledge but also fostering agency among marginalized populations to assert their privacy and data protection rights. They must aim to empower individuals and communities to engage meaningfully with privacy and data protection governance mechanisms, even in contexts of significant infrastructural and educational

limitations. This requires a commitment from governments and other stakeholders to develop inclusive frameworks that are responsive to these populations' socio-economic and cultural realities. Only through such comprehensive and inclusive measures can privacy education programs ensure equitable participation in privacy and data protection governance and protect the rights of all citizens, regardless of their access to technology or literacy levels.

Furthermore, simplifying access mechanisms is critical to reducing bureaucratic hurdles, making it easier for individuals to obtain information about their data without facing delays or procedural obstacles. This is especially important in rural or under-resourced areas where conventional data access methods may be impractical. Moreover, the technological infrastructure supporting access to personal data should be tailored to the African context. Instead of relying on expensive, high-maintenance systems, African countries could adopt affordable, sustainable, and locally appropriate technological solutions. Mobile-based platforms, which are already widely used across the continent, provide a practical solution for enabling data access, even in areas with limited internet connectivity. This is where African-grown IT ingenuity can play a transformative role in addressing real challenges faced by Africans, leveraging local expertise to create solutions that are not only technologically effective but also socially and culturally relevant. For instance, locally developed platforms such as M-Pesa in Kenya, which revolutionized secure mobile payments, and Ushahidi,⁸²⁰ which enables crowd-sourced information sharing, illustrate the scalability and adaptability of mobile technologies in tackling region-specific issues. Such innovations highlight the potential for homegrown technological initiatives to redefine data governance frameworks in ways that resonate with African realities. Governments and private entities could collaborate

⁸²⁰ The Ushahidi Platform helps communities turn information into action with an intuitive and accessible crowdsourcing and mapping tool. By enabling the rapid collection, management, and analysis of crowdsourced data, Ushahidi empowers individuals, community groups, governments, activists, and organizations to create meaningful change (see: <https://www.ushahidi.com/>).

to develop mobile-based platforms that allow individuals to manage their data, monitor its usage, and report misuse in real time.

Policymakers should prioritize public-private partnerships to create accessible and secure mobile technologies for data protection. These tools must be designed to support multiple local languages and incorporate culturally relevant interfaces, ensuring accessibility for diverse populations. By integrating local languages and culturally resonant design features, such platforms could significantly enhance accessibility and make data protection rights more universal and responsive to Africa's diverse needs. In communal African societies, the concept of access extends beyond individualistic notions of data ownership and management.⁸²¹ It involves active participation in decision-making processes, cultural practices, and the broader social life of the community.⁸²² Ensuring access in the African context requires facilitating both individual engagement with personal data and communal involvement in how data is managed and utilized. Redefining the principle of access within African privacy and data protection frameworks demands more than simply adopting Eurocentric standards. It requires a critical reevaluation of how these standards can be simplified and adapted to address the unique challenges faced by African countries, particularly those related to resource constraints and infrastructural limitations. By embracing simplified processes and contextually tailored technologies, African countries can develop data protection frameworks that are more effective, inclusive, and culturally resonant. This presents a critical opportunity to leverage Africa's vast human resource capacity in the digital space to engineer homegrown digital solutions. By capitalizing on local expertise, innovative technologies can be developed to address the specific privacy and data protection needs of the continent. These solutions would not only be tailored to African realities but also foster

⁸²¹ Vansina, J., "Oral Tradition as History" (1985), University of Wisconsin Press.

⁸²² Ibid.

economic empowerment and technological self-reliance, reinforcing the continent's position as a leader in digital innovation.

5.3.4 Decentralizing Data Protection Mechanisms: A Community-Driven Approach

To address the need for simplification and contextual adaptation, enhancing the principle of access in African contexts can be achieved through the decentralization of data protection mechanisms. While the GDPR mandates the appointment of data protection officers and the establishment of directories, many African countries that have incorporated similar provisions into their national privacy laws have struggled with effective implementation. As discussed in Chapter 4, these regulations often exist only on paper, with enforcement hampered by resource limitations and infrastructural challenges. Given Africa's unique socio-cultural and economic landscape, a more tailored approach is required. Rather than centralizing data protection mechanisms at the national level, a decentralized model that operates at the community or local government level would be more appropriate. This model would involve providing services in local languages, ensuring that data protection measures are accessible and comprehensible to all community members. By decentralizing these mechanisms, data protection becomes more inclusive and relevant to African contexts, making the system accessible to people in their immediate environments. Such a model could effectively replace the traditional structure of a single national data protection office, resulting in a framework more aligned with the needs and realities of African societies.

This redefined principle of access complements the broader theoretical framework of this thesis, which challenges Eurocentric models of international law and advocates for systems that integrate Africa's diverse socio-cultural realities. By emphasizing decentralized, community-driven strategies, African privacy and data protection frameworks can promote equity, sustainability, and community empowerment. Privacy measures should not only be

effective but also culturally resonant. An illustrative example is the communal management of natural resources, such as water, land, and forests, in many African societies.⁸²³ These systems ensure that resources remain accessible to all community members, minimize and mitigate conflicts, and promote sustainable management. Similarly, certain communal data should be treated as a communal asset, with access regulated by principles that emphasize equity, transparency, and community participation. By embedding these principles into data protection frameworks, African countries can ensure that policies are aligned with the cultural norms and social structures that are prevalent across the continent. African countries face the challenge of engaging with global data economies while maintaining local sovereignty. Regional initiatives, such as those undertaken by the AU and ECOWAS, offer a foundation for balancing these competing needs.

In this context, countries such as Kenya, Rwanda, and South Africa have aligned their national data protection laws with international standards, including the EU's GDPR, to facilitate trade while maintaining sovereignty, as outlined in chapter 4 of the thesis. These countries have negotiated cross-border data transfer agreements that mandate adequate protections on both sides of the transfer. However, it is important to acknowledge that the proliferation of diverse national data regimes across Africa has been identified as a significant obstacle to digital trade and, by extension, the AfCFTA initiative. This fragmentation creates challenges in harmonizing cross-border data transfers and complicates compliance for businesses operating across multiple jurisdictions. To address these challenges, African countries can draw on regional frameworks to engage in international trade while ensuring that data protection laws reflect African cultural and social values. The development of a pan-African data protection framework, aligned with international trade agreements but flexible

⁸²³ Unks, R. R. et al., "Diffuse Land Control, Shifting Pastoralist Institutions, and Processes of Accumulation in Southern Kenya" (2023) 50(5) *The Journal of Peasant Studies* 1757-1790, and Ameso, E. A. et al., "Pastoral Resilience among the Maasai Pastoralists of Laikipia County, Kenya" (2018) 7(2) *Land* 78.

enough to incorporate local governance structures, could serve as a model for balancing these competing interests. This would enable African countries to assert their sovereignty in data governance while participating in global digital markets. To ensure the effectiveness of decentralized, community-driven data protection frameworks, African countries can build on models already embedded in local governance systems. For example, in countries like Ghana and Nigeria, traditional leadership structures, including chiefs and community elders, could serve as local privacy councils responsible for adjudicating privacy-related disputes.⁸²⁴ These councils could collaborate with national data protection authorities to ensure that community-level concerns are addressed while maintaining alignment with national standards. The selection of council members could follow established local procedures for appointing representatives, ensuring inclusivity and trust in the process. Furthermore, these councils could liaise with national data protection officers to submit local data concerns and offer input on how national frameworks should be adapted to regional practices. This system would strike a balance between local autonomy and national and international regulatory compliance, facilitating a more flexible and culturally relevant data protection framework.

The success of such councils, however, would depend on the training provided to community leaders, particularly in navigating the evolving environment of digital privacy and data governance. Governments and civil society organizations should invest in capacity-building initiatives to ensure that local privacy and data protection councils are equipped with the necessary knowledge and tools to make informed decisions about data protection. While African countries must develop privacy and data protection frameworks that resonate with local cultural values, it is equally important that these frameworks engage effectively with the global data economy. African states should actively participate in international discussions on privacy and data protection to ensure that their perspectives are considered in shaping global

⁸²⁴ Lauren Honig, “Traditional Leaders and Development in Africa” (23 May 2019) Oxford Research Encyclopedia of Politics.

privacy and data protection norms. At the same time, African policymakers must advocate for data sovereignty, ensuring that any engagement with international frameworks, such as the GDPR, includes provisions for adaptation to local contexts. In this regard, the AfCFTA Protocol on Digital Trade presents a significant opportunity to align regional and global digital trade priorities with African data governance strategies. This Protocol, which seeks to harmonize digital trade regulations across the continent, can serve as a platform for African states to negotiate cohesive regional data transfer agreements. Such agreements would reflect communal values and facilitate the cross-border movement of data in ways that respect both international trade obligations and local governance structures. By utilizing the AfCFTA framework, African countries can ensure that regional cooperation strengthens their bargaining position in global discussions.

5.4 Data Stewardship in African Communal Contexts: A Model for Privacy and Protection

The global discourse on privacy and data protection frequently neglects the distinct cultural contexts and communal structures that define African societies. While frameworks like the GDPR offer comprehensive guidelines for data protection, they are primarily rooted in Western, individualistic values.⁸²⁵ In contrast, African societies are built on principles of collective ownership and stewardship, which require a fundamental re-evaluation of privacy and data protection models to align with these cultural realities.⁸²⁶ This thesis has consistently highlighted the need to incorporate such principles into privacy and data protection frameworks. Moreover, the concept of stewardship, deeply embedded in African traditions,

⁸²⁵ Greenleaf, G., “*Global Data Privacy Laws 2019: 132 National Laws & Many Bills*” (2019), Privacy Laws & Business International Report, 158, 22–30.

⁸²⁶ Prinsloo, P. & Kaliisa, R., “Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics” (2022) *Brit J Educ Technol* 53: 894-913.

offers a robust foundation for developing a culturally resonant and effective privacy and data protection framework.⁸²⁷

Expanding upon these principles, in African communal settings, stewardship profoundly shapes the approach to privacy and data protection. This concept is rooted in a cultural value system of care, responsibility, and accountability, extending beyond mere resource management to include the governance of personal and communal data.⁸²⁸ Stewardship in this context emphasizes the role of community members as active custodians of information, balancing the protection of individual privacy with the welfare of the community.⁸²⁹ Such stewardship involves a deep respect for communal data, upholding the principle that data practices should benefit the entire community equitably.⁸³⁰ This perspective views data not just as a resource, but as an integral part of communal life, deserving of protection to preserve cultural heritage and communal values. This approach contrasts sharply with more exploitative data practices that prioritize profit over communal welfare. In African contexts, data stewardship necessitates systems that ensure the confidentiality and integrity of both individual and communal information while also ensuring that the benefits derived from data are distributed fairly among all community members.⁸³¹ Stewardship in this sense does not merely protect data; it reinforces the community's role in governing data, fostering a balanced relationship where collective rights and benefits are prioritized.

This comprehensive approach to privacy and data protection resonates with the traditional roles of guardianship and custodianship that have been central to African societal structures for centuries. It reflects a commitment to managing data in a way that upholds

⁸²⁷ Owoniyi, S., "African Cultural Values: The Past, Present and Future", at 1–23.

⁸²⁸ Ibid.

⁸²⁹ Prinsloo, P. & Kaliisa, R., "Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics" (2022) *Brit J Educ Technol* 53: 894-913.

⁸³⁰ Ibid.

⁸³¹ Ibid.

individual rights while promoting communal well-being. In this context, data protection and privacy measures are grounded in local values of respect, interdependence, and reciprocity, ensuring that data functions as a tool for empowering and enriching the community rather than being exploited for personal gain. While the GDPR acknowledges the concept of stewardship through principles such as data minimization⁸³² and purpose limitation,⁸³³ the African communal context offers an additional dimension that further contextualizes privacy and data protection. The GDPR's approach emphasizes responsible data management by controllers and processors, ensuring data is collected and used only for legitimate and specified purposes.⁸³⁴ However, the African communal values of care, responsibility, and accountability extends this notion of stewardship beyond the individual or organizational level, embedding it within the broader community. By integrating this community-centric perspective, data protection and privacy measures in Africa can be further strengthened to align with local values of respect, interdependence, and reciprocity. This ensures that data serves as a tool for community empowerment and enrichment.

5.5 Colonial Influences on African Customary Law and Privacy Frameworks

Analyzing the historical backdrop of colonial influences on African customary law is essential for understanding the integration of cultural traditions with global privacy and data protection standards. This context illuminates how colonial legacies have shaped current legal frameworks and their alignment with traditional African values and practices. The European colonization of Africa has long impacted perceptions of African customary legal systems, often viewed through a Eurocentric lens.⁸³⁵ This perspective persists even in the realm of

⁸³² Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), "Recital 39 - Data Minimization and Purpose Limitation" (2016).

⁸³³ GDPR, art 5(1)(b).

⁸³⁴ Ibid.

⁸³⁵ Cobbah, J. A. M., *supra* note 674, "African Values and the Human Rights Debate: An African Perspective" (1987) 9(3) *Human Rights Quarterly* 309–331.

privacy and data protection laws, traditionally modelled on European standards.⁸³⁶ Initially, European legal studies expanded alongside colonial activities in the Americas and Asia, fostering a deeper self-awareness among Europeans about their cultural identity.⁸³⁷ During the colonial period in Africa, known as the Scramble for Africa, colonial powers faced the challenge of governing vast new territories.⁸³⁸ Due to limited resources and the difficulty of implementing foreign legal systems, colonial authorities were compelled to recognize and utilize African customary laws to some extent.⁸³⁹ This acknowledgment was often selective and reluctant, driven by practical needs rather than respect for African legal traditions.⁸⁴⁰ Moreover, certain aspects of African customary laws, such as polygamy, clashed with European ideals of civilized behaviour, creating further complexities.⁸⁴¹ The colonial strategy was to manage, rather than fully integrate, these traditional laws, resulting in a governance system continuously adapting to dynamic and orally preserved African customs.⁸⁴² From a TWAIL perspective, this selective recognition of customary law reflects the broader colonial strategy of legal subordination and epistemic domination. TWAIL scholars argue that colonial legal systems did not merely coexist with indigenous ones but actively undermined their legitimacy, reconfiguring them to serve the interests of the colonial state. This legacy continues to shape the structure and content of postcolonial legal orders, including privacy and data protection frameworks, which often privilege foreign regulatory models over local legal sensibilities.

Customary law, which often reflects established patterns of community behavior, plays a crucial role in defining norms that are expected to persist over time, potentially

⁸³⁶ Ibid.

⁸³⁷ Mamdani, M., *"Citizen and Subject: Contemporary Africa and the Legacy of Late Colonialism"* (1996), Princeton University Press.

⁸³⁸ Ibid.

⁸³⁹ Sandra F. Joireman, "Colonization and the Myth of the Customary" in Jeanmarie Fenrich, Paolo Galizzi & Tracy Higgins, eds, *The Future of African Customary Law* (2011), Cambridge University Press, 25-54.

⁸⁴⁰ Ibid.

⁸⁴¹ Ibid.

⁸⁴² Ibid.

evolving into formal obligations and duties.⁸⁴³ The recognition and integration of African customary laws into modern legal frameworks is vital for creating culturally relevant and effective data protection systems. Rather than imposing a uniform legal model, the coexistence of statutory laws with traditional and customary practices offers a more nuanced approach that better addresses the realities of African societies. This legal pluralism recognizes that African legal traditions are not static; they are dynamic, deeply embedded in community values, and capable of evolving in response to contemporary legal and societal challenges. TWAIL provides a powerful lens to critique the continued reliance on Eurocentric legal frameworks in the digital era. It calls for legal decolonization through the recovery of indigenous legal knowledge systems, including African privacy traditions, and demands that African states assert agency in defining normative standards that reflect their own socio-cultural realities. Rejecting the imposition of European legal standards as the sole framework for governance in African contexts, this perspective advocates for a more diverse and inclusive legal system that reflects the continent's rich legal traditions.

However, formalizing these practices into recognized legal obligations presents several complexities. Customary law, traditionally understood as fluid and evolving, may appear arbitrary to external observers. Historically, European legal scholars, shaped by positivist legal theories, have regarded law as emanating from sovereign authority and characterized by rational, intentional structures.⁸⁴⁴ In contrast, they often viewed customary law as informal and unstructured, more aligned with cultural practices than with formalized legal systems, thus relegating its study to anthropology rather than jurisprudence. The transcription of customary laws from oral traditions to written form introduced significant transformations, influenced not only by the process of documentation but also by the biases

⁸⁴³ Ibid.

⁸⁴⁴ Mamdani, M., *"Define and Rule: Native as Political Identity"* (2012), Harvard University Press.

of European authors involved.⁸⁴⁵ These authors often imposed their preconceptions and theoretical frameworks on the transcription process, which could distort the original intent and meaning of these laws. As a result, the challenges of recording and applying customary laws are emblematic of the broader colonial attitude toward African legal systems, characterized by a fundamental misunderstanding and underestimation of African legal traditions.⁸⁴⁶ This misapprehension affirms the complexities involved in integrating customary laws into contemporary legal frameworks. It calls for a more nuanced and respectful approach that recognizes the legitimacy, value, and evolving nature of African legal practices. Such an approach is essential for the creation of legal systems that are not only culturally appropriate but also reflective of the diverse legal traditions and values present across the continent.

Henceforth, integrating these historical perspectives into contemporary privacy and data protection frameworks in Africa requires recognizing and respecting the communal and fluid nature of African customary laws. As elaborated in this thesis, aligning these frameworks with traditional values involves overcoming the Eurocentric biases that have historically shaped African legal systems. By acknowledging the complexities and dynamics of African customary laws, policymakers can develop privacy and data protection policies that are culturally relevant and effective, thereby promoting self-determination and autonomy in the digital age. To address these historical biases and integrate African customary laws into contemporary legal frameworks, it is essential to understand the colonial perspectives that shaped current perceptions.

5.5.1 Colonial Perspectives on African Customary Law

⁸⁴⁵ Stephen Belcher, “Oral Traditions as Sources” in *Oxford Research Encyclopedia of African History* (2018).

⁸⁴⁶ Ibid.

The historical relationship between European colonial powers and their African colonies was characterized by authoritarian oversight and misguided paternalism.⁸⁴⁷ Major decisions were dictated from afar, resulting in a governance style aptly described as a ‘working misunderstanding.’⁸⁴⁸ This term still reflects the dynamics of customary law today. The earliest written records about African customary practices were created by outsiders, initially by Islamic scholars in the Sahel and Horn of Africa, and later by European colonists in the southern regions.⁸⁴⁹ These accounts were often biased, portraying African societies in an unfavorable light while occasionally acknowledging traits such as the dignity of warrior tribes like the Ashanti, Herero, and Zulu, or the esteemed traditions of pastoralists like the Khoe-Khoe, Masai, and Nuer.⁸⁵⁰ However, despite these positive portrayals, the prevailing colonial view condemned customary law as rigid adherence to tradition, often perceived as backward and unsophisticated.⁸⁵¹ This perspective was further reinforced by early anthropologists who argued that custom ruled as a tyrant in these societies, reflecting an inherent bias against what they termed ‘primitive societies.’⁸⁵² These societies were seen as spontaneous, tradition-bound, and lacking in rational and individual thought. In stark contrast, European legal systems were lauded for their rationality and progressiveness, designed as instruments of structured governance with clearly defined objectives. This dichotomy between European and African legal systems stressed the colonial powers’ view of African customary law as inferior.⁸⁵³ From a TWAIL perspective, this colonial construction of African customary law served a deeper political and ideological function. TWAIL scholars highlight how legal imperialism was central to the colonial project, not only through direct

⁸⁴⁷ Mamdani, *Define and Rule: Native as Political Identity* (2012), Harvard University Press.

⁸⁴⁸ Ibid.

⁸⁴⁹ T.W. Bennett, “Comparative Law and African Customary Law” in Mathias Reimann & Reinhard Zimmermann, eds, *The Oxford Handbook of Comparative Law*, 2nd ed (2019), Oxford University Press, 652-680.

⁸⁵⁰ Ibid.

⁸⁵¹ Ibid.

⁸⁵² Ibid.

⁸⁵³ Ibid.

imposition of foreign law but also through the systematic devaluation of indigenous legal epistemologies. Depicting African customary law as irrational or unsophisticated justified its marginalization and the imposition of Eurocentric legal frameworks. This process entrenched a hierarchy of legal knowledge, where Western norms were treated as universal and African traditions as local or outdated. TWAIL calls attention to this asymmetry, emphasizing that the colonial legacy in law was not just about governance, it was about the control of meaning, legitimacy, and legal authority.

However, understanding this historical context is crucial for shaping contemporary privacy and data protection frameworks in Africa. The imposition of Eurocentric legal principles, influenced by colonial biases, has often failed to account for the communal and fluid nature of African customary laws. These laws, grounded in consistent community behaviour and evolving norms, establish obligations and duties that are deeply intertwined with the social context of African societies.⁸⁵⁴ Yet, the transformation of these practices into formal legal obligations is complex, as traditional African customs often lack the rigid structure of Western legal systems. Moreover, the transcription of customary laws from oral to written form introduced significant alterations.⁸⁵⁵ European authors documenting these laws brought their biases and theoretical orientations, distorting the original intent and meaning of these laws.⁸⁵⁶ TWAIL offers an important corrective by foregrounding the need for epistemic justice. It asserts that African societies must not only reclaim their legal heritage but also be empowered to reshape legal frameworks in ways that reflect their own ontologies, values, and modes of social organization. This includes reconceptualizing data protection frameworks to align with African customary understandings of ownership, privacy, and communal responsibility. Rather than being viewed as incompatible with modernity, these

⁸⁵⁴ Belcher, S., "Oral Traditions as Sources" in *Oxford Research Encyclopedia of African History* (2018).

⁸⁵⁵ Ibid.

⁸⁵⁶ Mamdani, *Citizen and Subject: Contemporary Africa and the Legacy of Late Colonialism* (1996), Princeton University Press.

traditions should be seen as dynamic, adaptive, and capable of informing legal pluralism in a digitally connected age. By drawing on TWAIL, it becomes possible to critique the enduring Eurocentrism in African legal systems and to advocate for a more inclusive, decolonized approach to privacy and data governance, one that honours African customary law not as a relic, but as a living source of legal authority.

5.5.2 The Marginalization and Transformation of Customary Law in Colonial Africa

The 19th century marked a pivotal shift in the perception and application of customary laws in colonial Africa. The rise of legal positivism in Europe marginalized these laws, often dismissing them as incompatible with European concepts of statehood and sovereignty.⁸⁵⁷ As colonial powers imposed their legal paradigms in Africa, customary laws were sidelined, selectively recognized, and subjected to European standards of justice, equity, morality, and public policy.⁸⁵⁸ This selective application reinforced a system that privileged European rights and freedoms, significantly altering the original intent and meaning of African customary laws. Customary laws, dynamic and oral, were transcribed to fit European-style legal systems, introducing biases that distorted their application and undermined their cultural authenticity.⁸⁵⁹ The selective recognition of customary laws during the colonial era has profoundly influenced contemporary African legal systems. This colonial legacy perpetuates a fragmented legal environment where customary laws, despite their cultural significance, are often overshadowed by statutory frameworks imposed during colonization.⁸⁶⁰ Such fragmentation is particularly evident in the field of privacy and data protection, where tensions persist between culturally embedded communal values and globally dominant

⁸⁵⁷Ibid.

⁸⁵⁸ Ibid.

⁸⁵⁹ Belcher, S., "Oral Traditions as Sources" in *Oxford Research Encyclopedia of African History* (2018).

⁸⁶⁰ Chanock, M., *Law, Custom, and Social Order: The Colonial Experience in Malawi and Zambia* (1985), Cambridge University Press.

Eurocentric frameworks.⁸⁶¹ These tensions highlight the need to harmonize customary and modern legal systems to create privacy and data protection frameworks that genuinely reflect the realities of African societies.

To critically engage with this dynamic, the TWAIL framework offers a valuable lens. TWAIL highlights that the colonial reordering of legal systems was not incidental, but part of a broader project of legal imperialism, one designed to assert foreign dominance by displacing and delegitimizing indigenous governance systems. Through selective codification and the imposition of external legal hierarchies, colonial authorities subordinated African legal consciousness and embedded structural inequalities that persist to this day. TWAIL thus moves beyond description to critique, urging scholars and policymakers to foreground epistemic justice by re-centering African legal knowledge and values in contemporary reform efforts. Addressing this tension requires recognizing that data in African societies is not merely a collection of individual informational fragments but a representation of collective knowledge, history, and identity deeply embedded in social and cultural contexts. Governance mechanisms must reflect this duality, balancing the communal ownership of data with the protection of individual privacy rights. One example of this harmonization can be seen in Botswana's dual legal system, where customary law operates alongside statutory law in civil matters, including those related to land tenure and inheritance.⁸⁶² Customary courts, presided over by local chiefs, adjudicate disputes in ways that reflect traditional values and communal norms. This co-existence of legal systems offers a practical illustration of what TWAIL envisions as meaningful legal pluralism, one where indigenous systems are not merely tolerated but empowered to shape substantive outcomes. This model offers a potential blueprint for privacy and data protection frameworks, allowing the establishment of local

⁸⁶¹ Ibid.

⁸⁶² Martin Adams, *Land Tenure Policy and Practice in Botswana: Governance Lessons for Southern Africa*, (2003) Natural Resources Institute, University of Greenwich.

privacy councils that can adjudicate data-related disputes at the community level, ensuring that decisions reflect communal values while remaining consistent with national and international laws.⁸⁶³

However, TWAIL emphasizes that true transformation requires more than institutional reform; it requires a shift in how we conceptualize law, governance, and authority. From an African perspective, data governance must account for the collective ownership and stewardship of informational assets, extending beyond transactional frameworks to recognize cultural and spiritual dimensions. Sacred sites, cultural practices, and oral traditions hold significant informational value that transcends the individual and is deeply rooted in the collective experience. For instance, governing access to data about cultural heritage sites must respect the community's collective autonomy and ensure alignment with traditional values. The historical marginalization of customary laws highlights broader colonial dynamics of power and control. TWAIL situates this marginalization within a global system that privileges Western legal norms while silencing others, and it calls for the active restoration and empowerment of non-Western legal orders. In the context of privacy and data protection, this means reimagining legal frameworks that are not merely inclusive of customary norms but built upon them.

By addressing this legacy, African societies can foster privacy frameworks that are both culturally relevant and legally sound, promoting autonomy and inclusivity in the digital age. To achieve this, integrating African customary laws into contemporary legal frameworks requires a nuanced understanding of their socio-cultural contexts and inherent dynamism. Customary laws evolve in response to changing societal conditions, and their integration into privacy and data protection frameworks must embrace this fluidity. This involves codifying principles of collective ownership and stewardship within statutory law, ensuring that

⁸⁶³ Ibid.

governance mechanisms reflect African epistemologies while maintaining alignment with global privacy and data protection standards. In this sense, TWAIL does not only offer critique but also a roadmap for a decolonized legal future, one that respects local epistemologies while engaging critically with global standards. By prioritizing culturally informed approaches, this harmonization fosters trust, inclusivity, and autonomy, enabling privacy and data protection frameworks to genuinely reflect the lived experiences and values of African communities.

5.6 Addressing Economic Disparities and Resource Constraints in Data Protection for African Countries

The diverse economic context across African countries presents significant challenges in implementing GDPR-standard privacy and data protection measures. The punitive provisions of the GDPR, particularly the substantial fines for non-compliance, place a disproportionate burden on SMEs that dominate the African economic sector, as discussed earlier in this thesis. The economic strain that accompanies compliance with European data protection models highlights broader inequities inherent in global economic relationships. Many African countries, still grappling with the long-term economic consequences of colonial exploitation,⁸⁶⁴ face significant barriers in meeting the high-cost compliance standards imposed by frameworks like the GDPR.⁸⁶⁵ The reliance on trade relationships with European countries often forces African countries to adopt these stringent standards, even when they are economically unfeasible or poorly aligned with local conditions. This dynamic perpetuates a cycle of economic dependency, stifling the development of indigenous legal and regulatory systems that could more effectively address African realities and priorities. The risk of severe economic repercussions highlights the need for the development of

⁸⁶⁴ Rodney, W., *“How Europe Underdeveloped Africa”* (1972), Bogle-L'Ouverture Publications, 253-254.

⁸⁶⁵ Prinsloo, P. & Kaliisa, R., *supra* note 668, “Data Privacy on the African Continent: Opportunities, Challenges, and Implications for Learning Analytics” (2022) *Brit J Educ Technol* 53: 894-913.

regulatory frameworks that are not only effective but also flexible and scalable according to the varying economic capacities found across the continent.

These frameworks should be responsive to local contexts to avoid reinforcing existing power imbalances. Addressing these issues requires a critical recognition of the unique economic disparities across the African continent. For example, while countries such as South Africa and Nigeria benefit from robust economic hubs capable of supporting sophisticated cybersecurity infrastructures,⁸⁶⁶ other countries like Burundi and Malawi face extreme resource constraints and struggle to implement even basic data protection standards.⁸⁶⁷ These stark economic disparities significantly affect the feasibility and effectiveness of data protection policies across Africa.⁸⁶⁸ As such, there is an urgent need to develop solutions that are adaptable to both affluent and resource-limited contexts. A truly effective privacy and data protection framework for Africa must recognize and accommodate the continent's economic diversity, ensuring that it can be implemented in a manner that is both sustainable and equitable across different regions.

In addressing these challenges, a tiered approach to data protection regulation emerges as a promising solution. This approach would account for the varying sizes and capacities of data-handling entities, offering a balanced and inclusive model. Smaller businesses with limited resources would receive the support they need, while larger, more capable enterprises would be subject to stricter requirements. However, it is critical to acknowledge and safeguard against the possibility of this system being undermined through corporate structuring or deliberate fragmentation of larger enterprises into smaller entities to evade stricter requirements. To mitigate this risk, the framework must include provisions for periodic audits and robust oversight mechanisms to ensure compliance. Additionally, clear

⁸⁶⁶ Greenleaf, G., *"African Data Privacy Laws: Implications of Legal and Economic Disparities"* (2019), Privacy Laws & Business International Report, 158, 30–35.

⁸⁶⁷ Ibid.

⁸⁶⁸ Ibid.

criteria for determining the classification of data-handling entities should be established, taking into account factors such as corporate affiliations, shared ownership structures, and cumulative data-processing capacities. By adopting such a nuanced approach, African countries can effectively address the diverse economic realities that exist across the continent. Furthermore, innovative strategies that leverage open-source technologies, community-driven privacy and data governance models, and mobile-based solutions hold significant potential for overcoming economic barriers.⁸⁶⁹ These approaches can transform data protection from a potential burden into a powerful tool for empowerment, thereby enhancing trust and security within digital ecosystems. For example, utilizing open-source software for data protection offers a cost-effective method for implementing and customizing solutions, allowing strategies to be tailored to specific needs without incurring the high expenses associated with proprietary alternatives.⁸⁷⁰

Traditional community structures also play a crucial role in managing and safeguarding data, particularly in rural or underserved regions. Community-driven privacy and data governance models, which harness local knowledge and practices, can integrate data protection processes seamlessly into community life. This approach not only enhances the relevance and compliance of such measures but also ensures that they resonate with and empower the local population. For instance, communal resource management practices in African societies, such as those governing access to water, land, and forests, serve as valuable models for privacy and data protection frameworks.⁸⁷¹ These practices, which ensure equitable access and sustainable use, reflect the collective ownership and stewardship principles central to many African societies. By embedding these principles into data

⁸⁶⁹ Nneka Adaobi Ochuba et al, “Innovations in Business Models through Strategic Analytics and Management: Conceptual Exploration for Sustainable Growth” (2024) 6:3 *International Journal of Management & Entrepreneurship Research* 554-566.

⁸⁷⁰ Ibid.

⁸⁷¹ Naidoo, J., “Namibia's Community-Based Natural Resource Management Program: The Politics of Communal Land Tenure and the Management of Local Natural Resources” (2011).

protection policies, African countries can develop frameworks that are both culturally relevant and effective in safeguarding data.

5.7 Conclusion

This chapter has emphasized the critical importance for African countries to develop privacy and data protection frameworks that are firmly anchored in their distinct cultural, social, and economic contexts. The reliance on Western-centric models, particularly the GDPR, often fails to align with the communal values and collective identity that underpin many African societies. Therefore, a fundamental shift is required towards approaches that reflect local traditions and social realities, creating systems that are culturally congruent and contextually relevant. A key argument presented here is the need to align regulatory frameworks with the unique cultural and social structures of African communities. Unlike the predominantly individualistic orientation of many Western models, African cultures prioritize community, collective ownership, and shared responsibilities. This distinction calls for a departure from frameworks that exclusively prioritize individual rights, towards models that integrate communal perspectives, ensuring that data protection serves both individual and collective interests.

The chapter advocates for a culturally contextual approach, integrating traditional African values and communal practices into regulatory frameworks. Moving beyond the mere adoption of external legal standards, this approach encourages the development of indigenous frameworks that respect local customs and societal norms. By doing so, privacy and data protection regulations are more likely to resonate with the communities they are designed to protect, thereby ensuring both effectiveness and sustainability. Central to this approach is the principle of collective ownership and stewardship, which has long been a cornerstone of African societies. Applying this principle to data protection suggests that data,

akin to other communal resources, should be managed in a way that benefits the entire community. Data stewardship, in this context, emphasizes the role of community members and local authorities as custodians of data, ensuring its ethical use and protection. This model not only aligns with traditional African practices but also addresses the limitations of individualistic data protection frameworks that dominate global discourse.

The chapter further reinforces the importance of decentralized and community-driven data protection mechanisms. Rather than centralizing data governance at the national level, localized and community-based structures are proposed as more effective for ensuring compliance and building trust. These decentralized models, embedded within community structures and provided in local languages, are more accessible and culturally relevant, thereby enhancing their overall effectiveness. Furthermore, to accommodate the diverse legal and cultural contexts within African societies, the concept of legal pluralism, where multiple legal systems coexist, is proposed. This approach allows for the integration of customary laws with formal legal frameworks, creating a more inclusive and adaptable regulatory environment. Additionally, polycentric governance, with its multiple levels of authority, enhances the effectiveness of data protection frameworks by ensuring that local needs and practices are addressed appropriately.

Economic disparities across African countries also necessitate scalable and adaptable data protection strategies. This chapter advocates for tiered regulations that account for the varying capacities of different entities, coupled with the use of open-source technologies and community-driven governance models. These strategies aim to mitigate the economic challenges and resource constraints that many African countries face, transforming data protection from a potential burden into a tool for empowerment, trust-building, and security within digital ecosystems. A notable argument advanced in this chapter is the call for a significant shift away from Western-centric privacy and data protection models towards

frameworks that are culturally and contextually suited for Africa. By incorporating principles of collective ownership, stewardship, legal pluralism, and polycentric governance, and by addressing the continent's economic realities and resource limitations, African countries can develop robust, effective, and sustainable data protection strategies.

In conclusion, this chapter has illustrated the necessity for African countries to create privacy and data protection frameworks that are deeply rooted in their cultural, social, and economic contexts. It is evident that direct transplantation of Western models, like the GDPR, which prioritize individualistic values, often fails to resonate with the collective and communal realities that characterize African societies. By drawing on Indigenous concepts such as Ubuntu, communal land ownership traditions like those of the Maasai, and governance systems such as Ghana's chieftaincy structure, this chapter imagines the potential for extrapolating and adapting this African socio-cultural and philosophical ethos in the privacy and data protection sphere. This approach emphasizes how these traditions can inform a community-centred framework that acknowledges the importance of collective data ownership and stewardship, providing innovative pathways to address modern privacy challenges in a culturally relevant manner. The need for decolonization is also central to this discussion. African countries must resist the pressure to adopt Eurocentric frameworks that perpetuate global power imbalances and fail to align with local realities. Instead, the continent should embrace legal pluralism, where customary laws and modern statutory frameworks coexist, ensuring that privacy frameworks are both culturally relevant and legally effective. Initiatives such as the AU Convention on Cyber Security and Personal Data Protection provide a promising blueprint for harmonizing regional efforts and asserting Africa's sovereignty in the global data governance landscape.

The decentralization of data governance, through the establishment of Data Stewardship Councils and other community-driven mechanisms, presents a viable solution

for addressing the diverse needs of African societies. These councils would empower local communities to manage their data, ensuring that both individual privacy rights and collective responsibilities are respected. The potential of mobile technology and low-tech solutions like USSD platforms to bridge the digital divide and enhance access to privacy protection in regions with limited infrastructure is also emphasized in this chapter. Ultimately, for African countries to thrive in the global data economy while maintaining their sovereignty, there is an urgent need to create flexible, adaptable privacy frameworks that reflect African values, traditions, and governance systems. These frameworks must strike a balance between engaging with global data protection standards and ensuring that local norms are preserved. By doing so, African nations can secure data sovereignty and ensure that their citizens' privacy rights are safeguarded in a manner that is both meaningful and sustainable.

Chapter 6: Conclusion, Research Implications, and Policy Recommendations

6.0 Introduction

The rapid digital transformation and growing internet access across Africa have exposed significant shortcomings in the region's privacy and data protection regulatory frameworks. While these advancements have propelled the continent into the digital era, existing legal structures remain inadequate in safeguarding the privacy rights of African digital users, necessitating comprehensive reform. Globally, the GDPR has emerged as the leading standard for data protection since its implementation in 2018. However, it is crucial to recognize that the GDPR was developed within a European legal, economic, and cultural context, without input from African states during its formulation. Despite efforts by the AU, individual African countries, and RECs to develop their own privacy regulations, the GDPR's influence remains pervasive. This is largely due to its extraterritorial provisions, which condition African access to the EU market on GDPR compliance, reinforcing the region's economic and regulatory dependence. Furthermore, the persistence of GDPR-driven regulatory transplants reflects broader historical hierarchies in global governance, where African states continue to engage with international legal norms from a position of constrained agency. As a result, African countries often find themselves pressured to align their national privacy and data protection frameworks with EU standards, including the establishment of national privacy and data protection authorities modelled after those in the European Union. However, despite these efforts, the effectiveness of such measures remains limited due to their failure to integrate localized governance traditions, economic constraints, and indigenous legal principles.

Emerging regional mechanisms, such as the AfCFTA Protocol on Digital Trade, signal a potential shift in Africa's regulatory trajectory. By creating a unified African digital economy, the AfCFTA could provide an alternative framework for regional data governance, allowing African states to collectively negotiate privacy standards that are responsive to their economic and social realities. However, the extent to which such regional initiatives will successfully counterbalance GDPR dominance remains uncertain. The challenges posed by GDPR transplants reflect a broader phenomenon of data colonialism, where control over African data flows is dictated by external legal and economic forces. The geopolitical dimensions of the digital age have further exposed African countries to exploitation by international actors, exacerbating vulnerabilities created by weak privacy and data protection frameworks. Consequently, these challenges emphasize the urgency for African countries to move beyond simply replicating foreign models and instead focus on developing privacy and data protection regulations that are informed by local realities and tailored to the continent's diverse governance environments.

In light of these complexities, this thesis, titled "Beyond GDPR: Culturally Contextualized Privacy and Data Protection in Africa's Expanding Digital Landscape," critically examines three core issues:

1. The constraints and obstacles in implementing the GDPR in Africa, particularly concerning cultural compatibility, regulatory capacity, economic feasibility, and technological infrastructure.
2. The existing mechanisms, frameworks, and initiatives within Africa designed to address these regulatory concerns.
3. How privacy and data protection regulations can be tailored to reflect Africa's unique cultural, social, and economic factors.

Central to this thesis is the argument that privacy and data protection regulations in Africa must be specifically designed to reflect the continent's diverse cultural contexts and governance traditions. This argument is based on several key premises:

1. The African cultural framework emphasizes communal responsibility and collective identity, influencing how privacy and data protection should be structured.
2. The direct transplantation of Western privacy models, such as the GDPR, risks regulatory misalignment, as these frameworks prioritize individual autonomy over collective governance traditions.
3. The persistence of GDPR-driven policies raises concerns about regulatory sovereignty and the perpetuation of neocolonial legal structures that do not fully serve African interests.
4. Given these cultural, social, and economic disparities, a tailored approach to data protection in Africa is not only necessary but crucial. Such an approach would involve integrating community-based data governance structures, such as Data Stewardship Councils rooted in traditional authority systems, and developing tiered consent models that reflect varying levels of literacy and technological access. It would also entail codifying collective rights in data protection laws, particularly for sensitive cultural or communal information, and ensuring legal recognition of customary norms where appropriate.

This thesis argues that African states must adopt a decolonized approach to privacy and data protection governance. Rather than conforming to externally imposed regulatory models, African policymakers should develop frameworks that draw on indigenous legal principles, strengthen regional cooperation, and prioritize economic feasibility. By doing so, Africa can assert greater regulatory sovereignty while ensuring that privacy and data protection frameworks are both effective and culturally relevant.

6.1 Summary of the findings

6.1.1 Challenges of Implementing the GDPR in Africa

The GDPR has undoubtedly shaped global data protection norms, commended for its comprehensive focus on safeguarding user rights in the digital realm. However, its universalist approach assumes a level of institutional, economic, and legal uniformity that does not exist across all regions. This is particularly evident in Africa, where the GDPR's reliance on comprehensive regulatory enforcement mechanisms and well-resourced data protection authorities is at odds with the realities of most African states. The interwoven nature of today's digital economy reflects long-standing historical asymmetries, particularly the colonial imposition of European legal frameworks in Africa.⁸⁷² These legacies persist, shaping the way African countries interact with global regulatory norms. This regulatory dependence is evident in how contemporary European regulations, such as the GDPR, continue to dictate Africa's privacy and data protection regime.⁸⁷³ A primary challenge facing African states is the tension between regulatory sovereignty and economic dependence. The GDPR's extraterritorial provisions, which require compliance from any entity handling EU citizens' data, place African economies in a difficult position. This dynamic mirrors historical patterns where African economies were structured around European needs rather than domestic priorities.

In light of these findings, a critical question emerges: Can a uniform regulatory model, developed in a vastly different legal and economic context, adequately serve the needs of African societies? The GDPR's one-size-fits-all approach risks marginalizing the distinct legal, economic, and cultural realities of African countries. For example, privacy norms in

⁸⁷² Pourmokhtari, Navid, "A Postcolonial Critique of State Sovereignty in IR: The Contradictory Legacy of a 'West-centric' Discipline", 34:10 Third World Quarterly 1767-1793.

⁸⁷³ Ibid.

many African societies balance personal autonomy with community-based decision-making, a fundamental departure from the GDPR's individualistic legal foundation. Moreover, many African countries struggle with the financial and infrastructural demands of GDPR compliance. While the regulation assumes the presence of independent, well-resourced data protection authorities, the reality is that regulatory agencies in Africa often operate under severe constraints. For instance, while Ghana's Data Protection Act 843 and Kenya's Data Protection Act aim to align with international norms, enforcement challenges persist due to limited technical expertise, public awareness gaps, and underfunded regulatory bodies.

The GDPR's influence extends beyond legal transplants to shape Africa's digital trade relationships. For SMEs and emerging digital enterprises, GDPR compliance is often a financial and logistical burden, limiting their ability to scale and compete in global markets. Additionally, the disproportionate costs associated with compliance often result in smaller African businesses being excluded from international digital markets. This highlights the broader issue of digital sovereignty, where African states must navigate external regulatory impositions that prioritize European interests over localized economic and legal needs. The replication of GDPR-like frameworks in African jurisdictions has, in some cases, stifled the development of uniquely African approaches to data governance. For instance, regional frameworks such as the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) remain underutilized, as African states prioritize aligning with GDPR over strengthening continental data governance structures.

Despite these challenges, there are opportunities for African states to assert regulatory agency. For example, the AfCFTA Protocol on Digital Trade could serve as a platform for negotiating regional data protection policies that prioritize Africa's socio-economic realities. However, its success depends on fostering regulatory harmonization across jurisdictions, overcoming fragmentation, and investing in regional enforcement mechanisms. Ultimately,

this thesis argues that Africa must move beyond GDPR compliance as a default regulatory strategy. Instead of passively adopting European models, African states should prioritize the development of privacy and data protection frameworks that are tailored to their socio-legal, technological and economic environments. This shift requires a reorientation towards regulatory pluralism, where African legal frameworks integrate local knowledge systems, strengthen regional cooperation, and reduce external dependencies. By asserting regulatory independence, Africa can develop a privacy and data protection model that not only aligns with global best practices but also reflects the continent's diverse governance traditions, economic realities, and socio-cultural values.

6.1.2 Contextual Misalignment of GDPR with African Realities

This thesis has highlighted a fundamental misalignment between the European Union's GDPR and the socio-cultural and legal frameworks prevalent in African countries. In the European legal tradition, data protection is conceptualized as a distinct, standalone right, often treated separately from broader privacy concerns. This fragmentation contrasts with how privacy and data protection are understood in many African societies, where privacy is deeply interwoven with cultural traditions, communal values, and societal norms. Unlike the GDPR's emphasis on individual rights and self-determination, many African societies perceive privacy as a collective responsibility, where access to and control over information is governed through social structures rather than purely legalistic frameworks.

A key challenge in applying the GDPR in Africa is that its foundational principles emphasize individual autonomy, self-determination, and informed consent. However, in many African societies, privacy is often collectively negotiated rather than perceived as an isolated individual right. As a result, the GDPR's emphasis on personal control over data may not fully resonate in socio-legal contexts where decision-making is inherently communal. For

instance, in several African countries, privacy rights are not only embedded in societal expectations but are also enshrined in national constitutions, with specific provisions addressing data protection. However, even where legal protections exist, their enforcement is often inconsistent, and their alignment with cultural norms remains limited.

A key finding is that the GDPR's construction of the data subject as an autonomous individual sits in tension with relational ontologies prevalent in many African contexts. This divergence becomes visible across three linked pressure points central to data governance. First, identity: Recital 34 conceptualizes genetic and identity-related data in biomedical, individual terms, whereas information about one person can also implicate family, clan, or lineage; the privacy interest is therefore partly collective. Second, sensitivity and harm: building on that relational identity, Recital 51 frames special categories to protect individuals, yet disclosure of attributes such as health status, ethnic affiliation, or genetic disorders can generate stigma borne by households or communities; sensitivity thus has a relational dimension. Third, consent: in light of these relational stakes, Article 4(11)'s model of consent as a discrete, individual act often fails to reflect decision-making that is consulted or negotiated through familial or communal structures; this supplements rather than negates individual agency while preserving the individual's ability to object or withdraw. Taken together, these dynamics show why a strictly individual-rights model can misdescribe practice and why contextual adaptation is normatively and operationally necessary.

Despite the increasing prominence of privacy and data protection in African digital environments, African societies continue to uphold strong indigenous communal values that shape privacy perceptions. In traditional African governance systems, the regulation of personal and community data is often entrusted to elders, local councils, or tribal leaders who oversee access, use, and dissemination of information based on cultural protocols. This regulatory culture contrasts sharply with GDPR mechanisms, which place primary

responsibility on state institutions and independent data protection authorities. Thus, while scholars like Lee Bygrave have argued that African societies are evolving towards Western-style legal frameworks,⁸⁷⁴ the gap between formal legislative reforms and the deeply ingrained communal approach to privacy remains significant.

In light of these findings, a pivotal theme of this thesis is the necessity of contextualization, the adaptation of legal frameworks to align with Africa's unique cultural, social, and economic contexts. Rather than adopting a wholesale replication of the GDPR, African countries must critically evaluate which elements align with local realities and which require modification or supplementation. For example, legal norms in African societies tend to reflect a balance between individual and communal interests. Privacy and data protection frameworks must account for this balance to ensure cultural legitimacy and compliance. Given this evident misalignment, the one-size-fits-all approach exemplified by the GDPR proves unsuitable for the African context. This highlights the pressing need for an inclusive, adaptable, and culturally relevant privacy and data protection model, one that not only aligns with global standards but is also practically implementable across the continent.

While progress has been made toward regional data governance, efforts to implement culturally relevant privacy frameworks remain fragmented and largely advisory. For instance, the 2018 Personal Data Protection Guidelines for Africa, developed by the African Union Commission and the Internet Society, marked an important step toward recognizing regional privacy and data protection needs. However, despite their potential, these guidelines remain largely non-binding and lack enforcement mechanisms, limiting their effectiveness in reshaping national regulatory landscapes. The ongoing efforts to reform the African Union's Convention on Cyber Security and Personal Data Protection (Malabo Convention) present a significant opportunity to embed localized principles into a continental regulatory framework.

⁸⁷⁴ Bygrave, Lee A, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press, 2014).

Reforming the Malabo Convention to emphasize African-specific privacy governance approaches could mitigate the over-reliance on external regulatory models like the GDPR. However, progress remains slow, and without significant investment in regional enforcement structures, these efforts risk remaining aspirational rather than transformative.

Crucially, this process transcends the mere adoption of foreign legal models. Rather than engaging in reactive compliance with international norms, African countries must proactively shape regulatory policies that reflect their lived realities. Indigenous knowledge systems and governance structures must be integrated into formal privacy regulations to ensure their relevance, accessibility, and enforceability. By embedding these principles into national and regional frameworks, Africa can enhance both domestic regulatory legitimacy and its standing in global digital governance discussions.

6.1.3 Regulatory Burdens and Economic Implications

This thesis has illustrated the considerable economic challenges posed by the direct transplantation of the EU's GDPR in African countries. While the GDPR is recognized as a gold standard for data protection, its complex and resource-intensive compliance requirements impose a disproportionate burden on African economies, particularly SMEs, as detailed in Chapter 3. Given that SMEs constitute the majority of businesses in Africa, their ability to comply with such stringent regulations is significantly limited. As a result, rather than promoting economic growth and innovation, the GDPR's compliance requirements may inadvertently create barriers to participation in the digital economy for African enterprises. At the core of these challenges lies the issue of compliance costs, which unequally affect African businesses relative to their European counterparts. Specific compliance obligations under the GDPR, including mandatory data breach notifications, the appointment of Data Protection Officers, and extensive cybersecurity safeguards, necessitate substantial financial and technical investment. For African SMEs, which often operate within resource-constrained

environments, these obligations divert critical financial and human capital away from core business functions, ultimately stifling expansion and sustainability. Furthermore, the severe financial penalties for non-compliance, which can amount to 4% of global turnover, exacerbate these pressures. While designed to ensure compliance within the EU's economic landscape, such fines could cripple African enterprises, discouraging digital innovation and limiting entrepreneurial growth.

Another critical factor is the GDPR's extraterritorial scope. African businesses that process the personal data of EU residents must comply with the regulation, regardless of their geographical location. This imposes a dual compliance burden, forcing African businesses to adhere simultaneously to local data protection laws and the GDPR, creating substantial operational and legal challenges. The application of the GDPR beyond European borders not only reveals significant disparities in regulatory capacity between Europe and Africa but also highlights the inherent challenges of imposing a sophisticated legal framework on less developed economies. Furthermore, the GDPR's foundational principles are rooted in European legal traditions, which prioritize individual autonomy and personal data control. In contrast, many African societies embrace a collective approach to governance and data stewardship, where privacy rights are often understood within the framework of communal responsibility. As a result, the GDPR's focus on individual consent and self-determination may not fully align with Africa's broader cultural and social structures, where decision-making and resource-sharing are deeply interconnected within communities. This cultural divergence highlights the broader limitations of legal transplants, demonstrating that the uncritical application of foreign regulations can create significant misalignments with local economic, social, and legal realities. A major consequence of these dynamics is that the imperative to comply with the GDPR, largely driven by trade dependencies with the EU, has led many African governments to prioritize externally imposed frameworks over the

development of their own tailored data protection systems. This has contributed to a regulatory imbalance in which African states adopt stringent European standards that do not necessarily reflect the continent's diverse economic conditions, regulatory capacities, or digital infrastructure. Consequently, rather than fostering a regulatory environment that supports African digital economies, this approach constrains indigenous innovation, disempowers local businesses, and further entrenches Africa's economic dependency on external regulatory models.

6.1.4 The Necessity of Contextual Adaptation in Data Protection for Africa

The findings of this thesis affirm the urgent necessity for contextually adapted privacy and data protection frameworks in Africa. This thesis demonstrates that direct transplantation of foreign regulations, such as the GDPR, into African legal systems is not a sustainable approach unless carefully adapted to reflect the distinct cultural, legal, and economic contexts of African countries. While the GDPR is acknowledged as a comprehensive and robust regulation, its design is firmly rooted in European socio-legal structures, making its strict and uniform approach misaligned with the unique socio-economic realities of Africa. A significant issue identified by this research is the economic and regulatory pressure exerted by the GDPR on African countries, primarily due to the EU's role as one of Africa's largest trading partners. For instance, in 2021, the EU accounted for 23% of Africa's total trade, amounting to approximately 184 billion Euros, underscoring the continent's economic reliance on European markets. As a result, non-compliance with GDPR standards presents African nations with a risk of restricted trade access and economic penalties, reinforcing their dependency on European regulatory frameworks. However, the forced adoption of external regulatory standards without adapting them to local realities imposes burdensome requirements on African economies and restricts domestic policy flexibility.

This thesis argues that this dynamic can be viewed as a manifestation of regulatory imperialism, wherein the EU leverages the extraterritorial reach of the GDPR to dictate privacy standards globally, without adequately accounting for the socio-economic and cultural specificities of non-European nations, particularly in Africa. Consequently, African countries must actively assert their regulatory sovereignty by formulating data protection frameworks that are not externally imposed but are instead grounded in local governance traditions, economic priorities, and societal needs. Thus, Africa must move beyond passive adherence to foreign frameworks and actively construct a regulatory model that is responsive to its own realities. While maintaining engagement with global standards is important for international trade and cooperation, Africa's long-term data protection strategy must prioritize contextually adapted solutions that integrate legal pluralism, economic pragmatism, and cultural relevance.

Although the GDPR has set international benchmarks for data protection, its prescriptive and rigid nature limits its applicability in Africa's diverse digital ecosystems. Africa must engage with global data protection norms while simultaneously resisting the wholesale imposition of external legal regimes that fail to align with its local governance models and economic structures. For instance, European data protection laws emphasize individual rights and autonomy, whereas many African societies operate within collectivist traditions that balance individual privacy with communal obligations. As a result, African privacy and data protection laws must be designed to protect individual rights while simultaneously respecting and reinforcing the collective values embedded within African social structures. Developing an Africa-centric data protection model offers an opportunity to embed legal, economic, and social considerations that reflect the continent's priorities. This thesis emphasizes that African countries must adopt flexible and locally relevant data protection laws that balance economic imperatives with privacy rights, ensuring that their regulatory

structures serve both national interests and global engagement. Developing Africa-focused data protection laws would offer several benefits. First, it would allow African states to craft policies that align with their unique socio-economic landscape, reducing compliance burdens for SMEs and ensuring that businesses of all sizes can participate in the digital economy without being stifled by overly stringent regulations. Second, it would empower Africa to shape global data protection dialogues on equal footing, ensuring that its legal perspectives and economic constraints are acknowledged in international regulatory discussions.

6.2 Existing Mechanisms and Frameworks in Africa

The findings of this thesis emphasize that while significant strides have been made toward establishing a harmonized approach to privacy and data protection across Africa, persistent gaps remain in implementation, enforcement, and cultural alignment. Although the Malabo Convention and regional model laws have provided a starting point for regulatory development, their adoption remains inconsistent, and their substantive provisions still heavily reflect external legal influences, particularly European data protection norms. The thesis finds that the implementation of privacy and data protection laws remains uneven across Africa, with significant disparities between legal development and enforcement capacity. While some countries have fully operational data protection authorities, others lack the institutional capacity to monitor compliance effectively. This fragmentation hinders cross-border data flows, complicates intra-African digital trade, and weakens collective bargaining power in global digital governance discussions.

Moreover, existing regional frameworks, such as the Malabo Convention and REC model laws, remain largely underutilized and lack meaningful cultural contextualization. Many of these frameworks have borrowed extensively from the GDPR, emphasizing individual data rights without sufficiently incorporating African communal approaches to privacy and governance. Consequently, African states must move beyond merely replicating these

frameworks and instead focus on developing an indigenous regulatory approach that reflects both African economic realities and socio-cultural values.

6.2.1 Challenges of Harmonization and Enforcement

A key challenge highlighted in this thesis (Chapters 3 and 4) is the difficulty of harmonizing privacy and data protection laws across Africa. While significant progress has been made in developing regional data protection frameworks, such as the ECOWAS Supplementary Act and the SADC Model Law, the implementation and enforcement of these frameworks remain inconsistent across different jurisdictions. This inconsistency is exacerbated by disparities in legal traditions, economic development, and technological infrastructures, creating obstacles to achieving a cohesive and effective data protection regime. At the core of this challenge is the fact that privacy and data protection in Africa are often deeply rooted in constitutional provisions that guarantee the right to privacy. Unlike the GDPR, which treats data protection as a standalone legal right, African data protection laws frequently originate from and are intertwined with the right to privacy. Some African constitutions, in addition to recognizing privacy as a fundamental right, also provide for data protection explicitly. However, these constitutional guarantees do not always translate into effective enforcement mechanisms, resulting in a gap between legal recognition and practical implementation.

Despite growing legislative efforts, enforcement remains a significant weakness, as many countries lack the institutional capacity to oversee compliance effectively. The existing regional frameworks, such as the African Union's Malabo Convention, ECOWAS Supplementary Act, and the SADC Model Law on Data Protection, were designed to create a harmonized approach to data protection. However, this flexibility has also contributed to notable inconsistencies in how data protection regulations are implemented and enforced across different countries. A further challenge lies in the reliance on frameworks that lack

legally binding mechanisms, making enforcement weak and fragmented. While model laws provide guidance, they do not impose obligations, leaving significant gaps in compliance and accountability. The absence of binding frameworks with strong enforcement mechanisms complicates efforts to maintain compliance and consistency in data protection practices. As a result, cross-border data flows are hindered, and legal uncertainties emerge, particularly for businesses and individuals operating in multiple African jurisdictions. The challenge of harmonization, therefore, not only undermines the efficacy of data protection frameworks but also risks creating a fragmented legal environment where personal data is inadequately protected. For data protection to be effective across Africa, regional frameworks must evolve beyond advisory guidelines and include enforceable mechanisms that ensure compliance while accommodating national specificities.

One of the significant issues revealed in this thesis is the ineffectiveness of directly transplanting mechanisms from the GDPR into African legal systems, particularly in the establishment of Data Protection Authorities (DPAs). While the creation of DPAs mirrors the GDPR's framework, their enforcement across African countries remains largely superficial. In many instances, these regulatory bodies exist but lack operational capacity due to financial, technical, and human resource constraints. Many African countries face substantial resource constraints which severely limit the ability of these supervisory bodies to operate effectively. Even in relatively advanced economies, such as Nigeria and Ghana, DPAs struggle to conduct audits, monitor compliance, and enforce penalties effectively. Consequently, although numerous African countries have passed data protection laws and established DPAs, there is little evidence of strong enforcement, and non-compliance remains widespread. In some cases, DPAs have been established in law but have taken years to become operational, delaying the implementation of essential data protection safeguards. For example, in Mauritania, the DPA was established more than five years after the enactment of

the Data Protection Act, which meant that, during this period, data protection laws were in place without an entity to enforce them.

While South Africa's Information Regulator was established before the implementation of its POPIA, the early establishment of regulatory bodies does not necessarily guarantee strong enforcement. Even in countries with established DPAs, such as Nigeria and Kenya, the effectiveness of enforcement mechanisms remains questionable due to weak institutional capacity and budgetary constraints. For instance, Nigeria's Data Protection Bureau was created before its Data Protection Act was passed, leading to uncertainty about its jurisdiction and enforcement powers. The direct transplantation of European mechanisms, such as DPAs, without considering the specific socio-economic and legal conditions in African countries, has resulted in a gap between the formal adoption of laws and their practical enforcement. This misalignment highlights the ineffectiveness of simply replicating foreign models, such as the GDPR, without tailoring them to the realities on the ground. Rather than focusing solely on the establishment of DPAs, African governments should prioritize the capacity-building, funding, and operational independence of these authorities to ensure meaningful enforcement. In this regard, regional cooperation could play a crucial role in addressing enforcement challenges by facilitating the exchange of expertise, providing technical assistance, and harmonizing best practices. Strengthening DPAs through resource allocation and regional collaboration is critical for ensuring that privacy and data protection laws in Africa move beyond symbolic adoption and become practically enforceable frameworks.

6.2.2 The Dominant External Influence on African Data Protection Laws: A Continuation of Colonial Legacies

A critical insight drawn from this thesis is the significant external influence, particularly from Europe, on the development of data protection laws in Africa. While there have been some efforts to cultivate African-centered approaches, such initiatives remain overshadowed

by the pervasive reliance on foreign frameworks, especially those from Europe. The adoption of European models, particularly the GDPR, is largely driven by economic and legal pressures rather than a deliberate choice by African policymakers. While the adoption of established legal frameworks can be beneficial, the uncritical transplantation of GDPR-like regulations risks reinforcing historical patterns of external dependency. The extraterritorial reach of European laws, combined with Africa's economic reliance on European trade and investment, has led to the replication of EU privacy standards across the continent. The African Union's Convention on Cyber Security and Personal Data Protection, adopted in 2014, illustrates the broader challenge of asserting African autonomy in the development of privacy laws. Despite its potential to create a continent-wide, African-driven legal regime, it took nearly a decade to secure the necessary 15 ratifications for it to come into force in May 2023. The slow ratification process and the reluctance of many African countries to prioritize this convention reveal how regional coordination efforts have been weakened by the persistent influence of external legal frameworks.

More recently, the AfCFTA Protocol on Digital Trade has emerged as a potential mechanism for reducing reliance on European standards by fostering a more unified, intra-African approach to data governance. However, its success will depend on strong political commitment and the extent to which it integrates culturally contextualized privacy norms. Scholars such as Greenleaf and Cottier have observed that African privacy and data protection frameworks tend to replicate European models, particularly the GDPR. This replication is not merely incidental; it is reinforced by a broader economic and political system in which African countries remain intertwined with European powers. Beyond trade and economic incentives, European institutions have provided substantial financial and technical assistance to African countries in developing their data protection laws. However, this support comes with a subtle cost: the reinforcement of European-centric norms and

standards that do not fully account for Africa's cultural, legal, and socio-economic realities. This raises concerns about regulatory sovereignty, as African nations may find themselves compelled to comply with standards designed for vastly different legal and social environments. This thesis finds that the current regulatory landscape in Africa mirrors past colonial practices of legal transplantation, where European powers exported their legal systems to colonized territories with little consideration for the cultural and social frameworks that already existed. Today, this continues through the extraterritorial application of laws like the GDPR, which compels African countries to adhere to standards that were developed with European priorities in mind, not African ones.

While aligning with international standards is necessary for global digital trade, the challenge lies in ensuring that such alignment does not come at the cost of Africa's regulatory autonomy. In an attempt to counter these forces, initiatives such as the Network of African Data Protection Authorities have been established, aiming to promote privacy frameworks that reflect African realities. However, like many non-binding African-centered initiatives, their impact remains limited and symbolic rather than transformative. Without substantive institutional support or political will to challenge the prevailing dominance of foreign frameworks, these efforts may struggle to break the cycle of external influence that continues to define African legal development.

The findings of this thesis highlight the urgent need for Africa to assert greater control over its data protection frameworks. To achieve true regulatory sovereignty, African countries must craft data protection frameworks that not only comply with international standards but also resonate with the socio-cultural and economic dynamics unique to the continent. This involves embedding customary norms and communal governance principles into national legislation, facilitating community-based consultations during lawmaking, and establishing hybrid regulatory bodies that integrate traditional leadership with modern data governance

structures. It also requires investing in local capacity-building for data protection authorities, leveraging regional cooperation through bodies like the African Union and regional economic communities, and tailoring enforcement mechanisms to reflect local realities, including informal economies and low digital literacy rates. Otherwise, the persistence of external influences risks perpetuating Africa's marginalization in global governance, leaving African legal systems shaped by foreign priorities rather than by the needs and aspirations of African people.

6.2.3 African Philosophical Values and Data Protection Laws

The integration of African philosophical values into data protection laws remains a nascent area of inquiry, but one that is increasingly recognized as critical for creating sustainable regulatory frameworks. African legal systems are characterized by a unique form of legal pluralism, which blends customary norms with formal legal structures. This pluralism offers an opportunity for a potential reimagining of data protection frameworks in Africa that better reflect indigenous cultural values. Unlike the individual-centric conceptions of privacy found in European legal models, African societies often operate under relational and communalist philosophies, where collective well-being is prioritized over the primacy of individual rights. This philosophical distinction is crucial when considering the adaptation of privacy and data protection laws across the continent. One notable example is the concept of Ubuntu, a Southern African philosophy that emphasizes community, shared humanity, and human dignity. Ubuntu signifies interconnectedness and collective responsibility, which differs from the individual autonomy emphasized in frameworks such as the GDPR. While the GDPR establishes privacy as an individual right, Ubuntu conceptualizes privacy as a relational value, meaning privacy must be protected in a way that benefits both individuals and the broader community. There is growing academic support for the idea that Ubuntu could serve as a foundation for data protection laws that align with African social structures,

particularly in countries like South Africa. However, the extent of its application remains limited.

Despite the potential of African philosophies to shape data protection frameworks, existing laws largely mirror external models, particularly those inspired by the GDPR. Most African countries have opted to align their data protection laws with foreign standards, primarily those established by the EU. The limited incorporation of indigenous values into these frameworks highlights a significant gap in the legal development process, where local cultural norms are often overlooked or underutilized as a basis for regulatory design. This raises critical questions about the sustainability and effectiveness of such laws, particularly in societies where communal values are deeply embedded in the social structure. The findings of this thesis affirm the need for African countries to actively reassess the extent to which their data protection laws reflect indigenous philosophical values. A more inclusive approach that incorporates African legal pluralism and communalist principles could result in data protection frameworks that are not only legally robust but also culturally resonant, thereby fostering greater societal buy-in and compliance. Without such an approach, African data protection frameworks may remain disconnected from the lived realities of African societies, potentially undermining both compliance and enforcement.

6.3 The Need for Culturally Contextualized Adaptation in Privacy and Data Protection

As Africa's digital landscape rapidly expands, the challenge of implementing global data protection standards, particularly the GDPR, in African contexts has become increasingly complex. While the GDPR offers a robust framework for privacy and data protection, its one-size-fits-all approach often fails to take into account the deeply embedded particularities that shape African societies. In many African countries, the communal nature of society, rooted in collective values and indigenous traditions, stands in stark contrast to the individualistic

principles that dominate Western legal frameworks. As a result, the direct transplantation of the GDPR into African legal systems risks overlooking the continent's unique socio-economic conditions, potentially rendering these frameworks ineffective and difficult to enforce. Efforts by African countries to tailor data protection laws to local contexts have made notable progress, but these developments also highlight the ongoing need for a more culturally contextualized approach. South Africa's POPIA reflects an attempt to align international best practices with national priorities. POPIA incorporates important provisions that address South Africa's socio-economic history, particularly its legacy of inequality, by emphasizing protections for vulnerable populations. However, despite these advancements, POPIA remains anchored in a legal framework that draws heavily from the GDPR and continues to exhibit limitations in fully addressing South Africa's indigenous approaches to privacy and data governance. This reliance on global standards without deeper contextualization weakens its effectiveness.

Kenya's Data Protection Act (2019) similarly demonstrates an effort to balance the demands of a growing digital economy with the need for robust data protection measures. Unlike the GDPR, Kenya's law provides more flexibility in areas such as data localization and cross-border data transfers, reflecting the country's need for digital integration in the global market. This pragmatic approach recognizes local economic priorities while maintaining compliance with international data protection expectations. Yet, as with South Africa, Kenya's framework still does not fully address cultural norms around information sharing, privacy within families and communities, and collective data ownership. Rwanda, a leader in Africa's digital transformation, offers another example of a country striving to integrate data protection with national development goals. Its 2021 Data Protection and Privacy Law is designed to protect personal data while encouraging innovation in the tech sector. Although Rwanda's law aligns with its national development agenda, it still leans

heavily on GDPR-style provisions rather than developing an indigenous framework. Similarly, Ghana's Data Protection Act, enacted in 2012, serves as a foundational framework for data privacy in West Africa. Ghana's efforts to establish a Data Protection Commission and implement public awareness programs are commendable steps toward effective regulation. However, as with other GDPR-influenced laws, the deeper cultural contexts that underpin African societies are not fully integrated into these frameworks. These examples demonstrate that while African countries are making strides in adapting international data protection standards, the current efforts remain insufficient in addressing the complex and varied cultural and socio-economic contexts of the continent. More than simple modifications of the GDPR, Africa requires an entirely new regulatory approach rooted in the continent's legal traditions. This demands a shift away from the strictly individualistic paradigm that characterizes global standards toward a model that balances individual privacy rights with communal responsibilities.

African conceptions of privacy often frame personal data as a collective resource rather than an individual asset . Therefore, frameworks that fail to incorporate these perspectives risk being perceived as foreign impositions, which could hinder compliance and legitimacy. A culturally contextualized privacy and data protection framework for Africa must move beyond cosmetic legal modifications and engage deeply with the continent's long-standing governance traditions. Such a framework would embrace the collective ethos that defines many African societies and embed these values into the legal infrastructure. By doing so, African countries can create data protection systems that are not only aligned with international norms but also uniquely positioned to serve the interests of African people. This approach is crucial for ensuring that data protection laws are not only effective but also sustainable and widely accepted across Africa's diverse communities.

6.3.1 Recognition of Group and Collective Data Rights

A crucial aspect of this contextualized approach would be the recognition of group and communal data rights, beyond just individual rights. In many African societies, data is often considered a shared resource, owned collectively by families, clans, or ethnic groups rather than being solely an individual concern. For example, data generated by indigenous groups about their land, cultural practices, and genetic resources should not be treated as individual data under frameworks designed for Western-style privacy rights. These forms of communal data require stronger protection mechanisms that acknowledge the rights of groups, rather than focusing solely on the individual. African data protection frameworks should, therefore, introduce provisions that allow customary governance structures to play a role in regulating communal data, with clear protocols on how such data can be used, stored, or shared. This can be achieved by legally recognizing collective entities, such as councils of elders, community-based organizations, or cultural custodians, as data rights holders with the authority to grant or deny consent on behalf of the group.

Relational consent, as used in this thesis, differs procedurally and ethically from conventional informed consent. Procedurally, it records an individual's consent and, where the data implicate more than one person or a community, documents collective acknowledgment, for example, assent by designated group representatives or a brief community consultation, before processing proceeds. Ethically, it treats autonomy as interdependent rather than isolated, requiring attention to potential collective impacts, community welfare, and fair benefit-sharing alongside individual preferences. In short, relational consent supplements individual consent in African contexts by recognizing kinship ties, customary authority, and communal responsibility in decisions about personal and communal data.

National laws should include provisions enabling collective data stewardship, supported by a registry of communal data categories and group representatives responsible for managing access rights. For instance, certain cultural artifacts, oral traditions, and indigenous knowledge systems should not be freely commercialized or exploited by external entities without community consent. Protocols should be developed to establish community benefit-sharing agreements, impact assessments for data use involving communal resources, and mandatory consultation processes. Recognizing communal ownership of data could empower African societies to protect their cultural and intellectual heritage while still participating in the global data economy. This would also affirm the legal personality of collectives in data governance, enabling communities to pursue legal remedies when their collective rights are violated.

6.3.2 Traditional Dispute Resolution Mechanisms

Another significant adaptation would involve incorporating traditional African dispute resolution methods into data governance and privacy enforcement. Historically, African societies have used alternative dispute resolution (ADR) methods, such as mediation and negotiation through elders and customary courts, to resolve conflicts. These mechanisms emphasize collective accountability and relational justice, rather than punitive measures, which makes them particularly well-suited for addressing privacy breaches and data-related disputes. African data protection frameworks should formally recognize these mechanisms, allowing data protection disputes, whether between individuals, businesses, or government entities, to be resolved in a way that reflects local traditions of consensus-building and community harmony. This would be particularly relevant in contexts where legal literacy is low, and where navigating formal court systems is financially or logistically prohibitive. Creating localized, community-based data protection bodies that can adjudicate disputes

using these established methods would ensure that justice is accessible, culturally relevant, and reflective of African values.

6.3.3 Frameworks in Local Languages and Accessible Formats

An additional way to make privacy and data protection frameworks more culturally contextualized is by ensuring that legal frameworks are available in local languages and in formats that are comprehensible to diverse populations. Africa's linguistic diversity is immense, and many people communicate primarily in their native languages. However, most existing data protection laws in Africa are written in English, French, or Portuguese, limiting accessibility. Translating data protection laws and regulations into these local languages will enhance public engagement and enforcement, as people will have better access to legal recourse when their privacy rights are violated. Moreover, creating visual, audio, and interactive digital materials that are accessible to individuals with low literacy levels can help ensure that data protection is widely understood at the grassroots level. Harnessing radio programs, community workshops, and mobile-based tools in rural areas can further support privacy education efforts.

6.3.4 Contextualized Compliance Mechanisms

Recognizing the varying levels of technological and economic development across Africa, compliance mechanisms within data protection frameworks should be designed with graduated obligations rather than rigid one-size-fits-all requirements. SMEs, which form the backbone of many African economies, may struggle to meet the stringent compliance requirements influenced by the GDPR, such as appointing Data Protection Officers or implementing high-cost cybersecurity measures. African countries could implement scalable and tiered compliance obligations, allowing smaller businesses or those in rural or underserved areas to adopt privacy safeguards incrementally, while still adhering to basic

privacy safeguards. For example, a phased compliance structure could require large multinational corporations operating in Africa to meet full GDPR-level standards, while smaller businesses could begin with baseline requirements, such as obtaining informed consent for data collection. This approach would encourage greater adherence to data protection laws without placing an undue burden on innovation and entrepreneurship.

6.4 Implications of the Research

The findings presented in this thesis have far-reaching implications for the design and implementation of privacy and data protection frameworks in Africa. Through a critical examination of the complexities inherent in adopting the GDPR and a detailed analysis of the socio-cultural, legal, and economic realities unique to Africa, this thesis emphasizes the necessity for contextually relevant data governance strategies that are not merely regulatory transplants but reflect Africa's legal and economic sovereignty. The thesis emphasizes that a harmonized but flexible approach is critical for ensuring Africa's participation in the global digital economy while safeguarding privacy and data rights.

6.4.1 Contextualization of Privacy and Data Protection Frameworks

A key implication of this thesis is the need for privacy and data protection frameworks that align with Africa's historical, legal, and economic realities. By applying the TWAIL lens, this thesis highlights how contemporary privacy laws perpetuate historical hierarchies, positioning African states as passive recipients of Western norms rather than active participants in shaping global digital governance. This thesis argues that privacy and data protection in Africa must incorporate principles of collective digital sovereignty, recognizing that data governance is not solely an individual concern but one tied to national and regional development. Instead of adopting a one-size-fits-all approach modelled after the GDPR,

African data governance strategies must reflect the continent's economic structure, which relies heavily on SMEs, the informal sector, and digital trade.

6.4.2 Policy Development and Legal Reform

This thesis highlights the limitations of adopting global frameworks without careful adaptation and calls for a harmonized yet adaptable model of privacy and data protection, integrating existing regional efforts. This thesis recommends that African states negotiate common standards for cross-border data flows, ensuring that data localization requirements and compliance mechanisms do not stifle economic participation. Developing regionally coordinated mechanisms for privacy and data protection, rather than fragmented national policies, will enhance Africa's capacity to regulate data flows while promoting economic development. By embedding digital trade considerations into privacy and data protection laws, Africa can strengthen its economic sovereignty while promoting a rights-based approach to data governance. This approach requires capacity-building at the national level and the development of implementation mechanisms tailored to different economic contexts across the continent.

6.4.3 Contribution to Academic Discourse and Theoretical Development

By centering TWAIL as a critical analytical tool, this thesis challenges the dominance of Eurocentric data protection paradigms and highlights how international legal frameworks have historically marginalized African regulatory agencies. This research calls for greater academic engagement with African epistemologies in digital governance, advocating for a paradigm shift that positions Africa as a norm entrepreneur rather than a passive adopter of foreign regulations. This research also contributes to broader discussions on legal pluralism in global digital governance, emphasizing the need for international legal standards that reflect diverse regulatory approaches rather than reinforcing historical power asymmetries.

Africa's leadership in developing contextualized privacy laws can serve as a model for other Global South nations, demonstrating that regulatory sovereignty and digital economic growth can coexist.

6.5 Recommendations

This thesis emphasizes the necessity for a contextually tailored approach to privacy and data protection laws in Africa. While global frameworks like the GDPR have established baseline international standards, their direct transplantation into African legal systems, without consideration of regional economic, social, and cultural realities, is problematic. To ensure privacy and data protection laws are both effective and sustainable, Africa must develop frameworks that prioritize local needs while integrating international best practices. The following recommendations are designed to guide this effort.

6.5.1 Moving Beyond GDPR: Developing Culturally Relevant Data Protection Laws

African policymakers must avoid rigid transplants of GDPR-like models and instead develop legal frameworks that reflect Africa's unique digital landscape. While key principles such as transparency, accountability, and fairness remain essential, privacy and data protection laws must be adapted to align with African values, including collective well-being and communal rights. The AfCFTA Protocol on Digital Trade provides a strategic opportunity to harmonize regional data protection laws while enhancing intra-African digital trade. However, full legal harmonization across African states may not be immediately attainable, given the diversity of legal traditions, regulatory capacities, and stages of digital readiness across the continent. To navigate this complexity, a tiered approach to data protection is proposed as a more flexible and pragmatic alternative. Under this model, African countries could first adopt a shared set of minimum data protection principles, such as the rights to access, rectification, and informed consent, as a common foundation. Building on this baseline, individual countries would retain the autonomy to introduce context-specific rules

and mechanisms that reflect their distinct socio-cultural norms, economic structures, and technological capabilities. This graduated model would ensure that no country is left behind in the process of strengthening data protection while simultaneously allowing more advanced jurisdictions to pursue enhanced safeguards in line with their capacity. It encourages legal pluralism within a cohesive continental strategy, promoting both unity and diversity. Ultimately, Rather than viewing privacy and data protection as a purely legal obligation, African countries must integrate it into their broader economic and developmental strategies to support both privacy and data protection rights and digital entrepreneurship.

6.5.2 Regional Harmonization and Legal Cooperation

Achieving coherence in Africa's data governance framework requires regional cooperation through mechanisms such as the AU Data Policy Framework, REC initiatives, and the AfCFTA's digital trade agenda. African countries should establish regional regulatory alignment that facilitates cross-border data transfers while ensuring comprehensive protection mechanisms.

Key steps for harmonization include:

- Strengthening the AU's role in coordinating regional and continental data governance policies.
- Aligning national data protection laws with regional trade policies under AfCFTA to support digital innovation and economic growth.
- Ensuring practical enforcement through capacity-building programs and the creation of regionally coordinated compliance mechanisms.

A Pan-African Data Protection Body under the AU could serve as a central institution for coordinating data governance efforts, ensuring harmonization without imposing a rigid, one-size-fits-all framework.

6.5.3 Integrating African Cultural Values into Legal Frameworks

For privacy and data protection laws to be effective and widely accepted, they must resonate with Africa's communal structures and cultural values. Unlike the GDPR, which places individual autonomy at the center of privacy protection, many African societies view privacy as a collective concern.

To reflect African realities, privacy and data protection laws should:

- Recognize collective rights over data, particularly in cases of indigenous data ownership and communal governance.
- Ensure accessibility of privacy and data protection laws by translating them into local languages and making them understandable for rural communities.
- Promote decentralized enforcement by establishing regional and local privacy and Data Protection Authorities that are adapted to different social and economic contexts.

By embedding these cultural considerations into legal frameworks, Africa can develop privacy and data protection laws that are both practical and deeply rooted in local realities.

6.6 Conclusion and Future Pathways

As Africa navigates the complexities of an increasingly digitalized economy, this thesis emphasizes the urgent need for contextually relevant privacy and data protection frameworks. The research has demonstrated that directly transplanting foreign legal models, such as the GDPR, results in regulatory misalignment that fails to reflect Africa's diverse legal traditions, communal values, and economic structures. Instead, a tailored African approach and regional legal harmonization are essential for reclaiming Africa's regulatory sovereignty in global digital governance. The future of Africa's privacy and data protection regime must be shaped on Africa's terms, balancing global interoperability with local relevance. This requires harmonizing legal frameworks across the continent while ensuring data sovereignty and

economic resilience. By doing so, Africa can strengthen its position in the global digital economy while safeguarding individual and collective privacy rights.

6.6.1 Call to action

African policymakers must act decisively to establish privacy and data protection frameworks that are regionally integrated, flexible, and forward-thinking. These frameworks should:

- Utilize the AfCFTA Protocol on Digital Trade to develop harmonized, trade-friendly privacy and data protection laws that support digital innovation while ensuring privacy safeguards.
- Embed African cultural and legal traditions into privacy and data protection laws, ensuring that collective data rights and community governance structures are recognized.

Bibliography

1. A.B. Makulilo. African Data Privacy Laws. Law, Governance and Technology Series, vol. 33 (Springer International Publishing AG, 2016) at 198.
2. Abdulrauf, Lukman. Giving 'Teeth' to the AU Towards Advancing Compliance with Data Privacy Norms. *Information & Communications Technology Law* 30, no. 87 (2021): 88 et seq.
3. Abdulrauf, L. A., “African Approach(es) to Data Protection Law” (2024) in *Data Protection Law in Africa*, De Gruyter, 31–53.
4. Abdulrauf, L. A., “African Approach(es) to Data Protection Law” (2024) in *The Emergent African Union Law: Conceptualization, Delimitation, and Application*, 45.
5. Abdulrauf, L. A., “The African Union’s Data Protection Convention 2014: A Cause for Celebration of Human Rights in Africa?” (2014) 33–45.
6. Access Now, *Strengthening Data Protection in Africa: Key Issues for Implementation*.
7. Afolayan, Adeshina. *Individualism, Communitarianism and African Philosophy: A Review Essay on Exploring the Ethics of Individualism and Communitarianism*.
8. Africa Continental Free Trade Agreement (AfCFTA). Adopted 21 March 2018, entered into force 30 May 2019.
9. Africa Privacy Report 2023–2024. Lawyers Hub, 2023.
10. African Charter on Human and Peoples’ Rights. Adopted 27 June 1981, OAU Doc CAB/LEG/67/3 rev. 5, 21 ILM 58 (1982) (entered into force 21 October 1986).
11. African Charter on the Rights and Welfare of the Child. Adopted 11 July 1990, OAU Doc. CAB/LEG/24.9/49 (1990), entered into force 29 November 1999.
12. African Commission on Human and Peoples’ Rights, *Principles and Guidelines on Human and Peoples’ Rights while Countering Terrorism in Africa*. Part 11 (2015).

13. African Countries Are Building a Giant Free-Trade Area. 2017. Economist, December 7, 2017.
14. African Manners, Gikuyu Proverbs. African Manners, July 7, 2012.
<http://africanmanners.blogspot.com>
15. African Peer Review Mechanism, Africa Governance Report: Promoting African Union Shared Values (2021). African Peer Review Mechanism.
16. African Union Convention on Cyber Security and Personal Data Protection. African Union, 2014.
17. African Union Convention on Cyber-security and Personal Data Protection. 2014.
https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
18. African Union Data Policy Framework. Endorsed by the AU Executive Council, February 2022.
19. African Union, Agenda 2063. African Union (2024).
20. Ahmore Burger-Smidt. Enforcement Notice Issued to Dis-Chem Due to Contravention of POPIA, Werksmans Attorneys (18 September 2023).
21. Algeria, Law No 18-07 of 25 Ramadhan 1439 (10 June 2018) Relating to the Protection of Individuals in the Processing of Personal Data.
22. Ana Mishova. GDPR and Data Protection Laws in Africa: A Comparison (29 November 2023), online: GDPR Local.
23. Anand, S., & Ebras, D. “Data Colonialism: Rethinking Data Extraction and the Global South.” Global Perspectives (2023).
24. Anghie, Antony. 1996. Imperialism, Sovereignty, and the Making of International Law, Cambridge Studies in International and Comparative Law. Cambridge, UK; New York: Cambridge University Press.

25. Anu Bradford. "Exporting Standards: The Externalization of the EU's Regulatory Power Via Markets." *International Review of Law and Economics* 42 (2015): 158, 170.
26. Anu Bradford. "The Brussels Effect." *Northwestern University Law Review* 107 (2015): 1.
27. Babatunde Fagbayibo. "Exploring Legal Imperatives of Regional Integration in Africa." *The Comparative and International Law Journal of Southern Africa* 45, no. 1 (March 2012): 64–76.
28. Bakibinga, EM. *Regulating Market Entry in the Telecommunications Sector in an Integrated East Africa: Towards a Common Licensing Framework*. Master's thesis.
29. Banisar, D., & Davies, S. "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments." *J. Marshall J. Computer & Info. L.* 18 (1999): 1.
30. Banisar, D. "Linking ICTs, the Right to Privacy, Freedom of Expression and Access to Information." *East African Journal of Peace & Human Rights* 16, no. 1 (2010).
31. Belcher, S. "Oral Traditions as Sources." In *Oxford Research Encyclopedia of African History* (2018).
32. Bennett, T. W. "Comparative Law and African Customary Law." In Mathias Reimann & Reinhard Zimmermann, eds, *The Oxford Handbook of Comparative Law*, 2nd ed (2019), Oxford University Press, 652–680.
33. Boshe, Patricia, Moritz Hennemann & Ricarda von Meding. "African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward." *Global Privacy Law Review* 3, no. 2 (2022): 56–64.
34. Brehm, H. N., Uggen, C., & Gasanabo, J. D. "Genocide, Justice, and Rwanda's Gacaca Courts." *J Contemp Crim Just* 30, no. 3 (2014): 333–352.

35. British Academy, Royal Society & techUK. Data Ownership, Rights and Controls: Reaching a Common Understanding (2018).
36. Bygrave, Lee A. Data Privacy Law: An International Perspective. Oxford: Oxford University Press, 2014.
37. Bygrave, Lee A. “Data Protection Pursuant to the Right in Human Rights Treaties.” (1998) 6:3 International Journal of Law and Information Technology 247–284 at 283.
38. Bygrave, Lee A. “Privacy and Data Protection in an International Perspective.” (2010) 56 Scandinavian Studies in Law 165–200 at 193.
39. Bygrave, Lee A. “Privacy Protection in a Global Context—A Comparative Overview.” (2004) 47 Scandinavian Studies in Law 319–348 at 328.
40. Cara Mannion. “Data Imperialism: The GDPR’s Disastrous Impact on Africa’s E-Commerce Markets.” Vanderbilt Journal of Transnational Law 53, no. 2 (March 2020).
41. Caruana, MM, & Cannataci, JA. “European Union Privacy and Data Protection Principles: Compatibility with Culture and Legal Frameworks in Islamic States.” Information & Communications Technology Law 16, no. 2 (2007): 99–124.
42. Chad, Law No 007/PR/2015 on the Protection of Personal Data.
43. Chad, Ordinance No 002/PR/2019 Amending Act No 006/PR/2015 on the Creation of the National Agency for Computer Security and Electronic Certification.
44. Charter of Fundamental Rights of the European Union. 2000 O.J. (C 364) 1.
45. Chee, Foo Yun. 2019. “Yet to Show Its Teeth, Landmark EU Privacy Law Already a Global Standard.” Reuters, May 22, 2019.
46. Chimni, B.S. “Third World Approaches to International Law: A Manifesto.” Third World Quarterly 27, no. 5 (2006): 767–776.

47. Cobbah, Josiah A. M. "African Values and the Human Rights Debate: An African Perspective." *Human Rights Quarterly* 9, no. 3 (1987): 309–331.
48. Communauté Économique et Monétaire de l'Afrique Centrale (CEMAC). Established by the Treaty of N'Djamena, 16 March 1994, Central Africa.
49. Constitution of Algeria (1996).
50. Constitution of Angola (2010).
51. Constitution of Benin (1990).
52. Constitution of Botswana (1966).
53. Constitution of Burkina Faso (1991).
54. Constitution of Burundi (2018).
55. Constitution of Cape Verde.
56. Constitution of Chad (2018).
57. Constitution of Comoros (2018).
58. Constitution of Djibouti (1992).
59. Constitution of Egypt (2014).
60. Constitution of Eritrea.
61. Constitution of Ethiopia (1994).
62. Constitution of Gabon (1991).
63. Constitution of Gambia (1997).
64. Constitution of Guinea (2010).
65. Constitution of Guinea-Bissau (1984).
66. Constitution of Kenya (2010).
67. Constitution of Lesotho (1993).
68. Constitution of Liberia.
69. Constitution of Libya.

70. Constitution of Madagascar (2010).
71. Constitution of Malawi (1994).
72. Constitution of Mali (1992).
73. Constitution of Mauritania.
74. Constitution of Morocco (2011).
75. Constitution of Mozambique.
76. Constitution of Namibia (1990).
77. Constitution of Niger (2010).
78. Constitution of Nigeria (1999).
79. Constitution of Rwanda (2003).
80. Constitution of Sao Tome and Principe.
81. Constitution of Senegal (2001).
82. Constitution of Seychelles.
83. Constitution of Sierra Leone.
84. Constitution of Somalia (Provisional Constitution, 2012).
85. Constitution of South Africa (1996).
86. Constitution of South Sudan (2011).
87. Constitution of Sudan.
88. Constitution of Swaziland (2005).
89. Constitution of Tanzania (1977).
90. Constitution of the Democratic Republic of Congo (2005).
91. Constitution of The Gambia (Draft Constitution, 2019).
92. Constitution of the Republic of Congo (2015).
93. Constitution of Togo (1992).
94. Constitution of Tunisia (2014).

95. Constitution of Uganda (1995).
96. Constitution of Zambia.
97. Constitution of Zimbabwe (2013).
98. Constitutive Act of the African Union. Adopted 11 July 2000, entered into force 26 May 2001.
99. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). Council of Europe, opened for signature 28 January 1981, ETS No. 108 (entered into force 1 October 1985).
100. Council Regulation (EU) 2016/679 of the European Parliament and of the Council. 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 O.J. (L 119) 1.
101. Currie, I. “The Concept of Privacy in the South African Constitution: Reprise: Aantekeninge.” (2008) 2008:3 Journal of South African Law/Tydskrif vir die Suid-Afrikaanse Reg 549–557.
102. Dagbanja, Dominic N. 2001. “The Right to Privacy and Data Protection in Ghana.” In African Data Privacy Laws, edited by Alex B. Makulilo, 229–231.
103. Data Protection Act 2003 (Act No. 9 of 2003). Seychelles.
104. Data Protection Act 2011 (Act No. 5 of 2012). Kingdom of Lesotho.
105. Data Protection Act 2017 (Act No. 22 of 2017). Mauritius.
106. Data Protection Act 2018 (Act No. 18 of 2018). Kingdom of Eswatini.
107. Data Protection Act 2018 (Act No. 32 of 2018). Botswana.
108. Data Protection and Privacy Act, 2019 (Act No. 9 of 2019). Uganda.
109. Data Protection Bill 2021. Zambia.

110. Deepening African Integration: Intra-African Trade for Development and Poverty Reduction. 2016. African Perspectives on Trade and the WTO, 11–11.
doi:10.30875/e5b1e7e1-en.
111. Directive 95/46/EC of the European Parliament and of the Council. 1995. “On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.” 1995 O.J. (L 281) 31.
112. Directive C/DIR. 1/08/11 on Fighting Cybercrime within ECOWAS. Issued August 2011.
113. DLA Piper Africa. “New Hurdles to Transferring European Personal Data to Mauritius.” (No year given.)
114. East African Community (EAC). Established by the Treaty for the Establishment of the East African Community, signed on 30 November 1999, entered into force on 7 July 2000.
115. Economic Community of Central African States (ECCAS). Established by the Treaty of Libreville, 18 October 1983.
116. Economic Community of West African States (ECOWAS). Established by the Treaty of Lagos, 28 May 1975.
117. Egypt, Law No 151 of 2020 on the Protection of Personal Data. Ratified on 13 July 2020 by President Abdel Fattah al-Sisi.
118. Enforcementtracker. “Statistics: Fines Imposed Over Time,” accessed 20 April 2024.
119. Equatorial Guinea, Law No 1/2016 on the Protection of Personal Data.
120. Eslava, Luis, and Sundhya Pahuja. “Beyond the (Post)Colonial: TWAIL and the Everyday Life of International Law.” *Verfassung und Recht in Übersee / Law and Politics in Africa, Asia and Latin America* 45, no. 2 (2012): 195–221.

121. Etta, Emmanuel E., Dingba Dingba Esowe & Offiong O Asukwo. 2016. "African Communalism and Globalization." 10:3 African Research Review 302.
122. European Commission. "Adequacy Decisions," European Commission – European Data Protection. (No date given.)
123. European Data Protection Board. 1.2 Billion Euro Fine for Facebook as a Result of EDPB Binding Decision. (No year given.)

European Data Protection Board. The European Data Protection Board (last updated 6 April 2022).
124. European Data Protection Supervisor. "The History of the General Data Protection Regulation."
125. European Parliament and Council of the European Union. "Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data..." Official Journal of the European Union L 119 (2016): 89–131.
126. European Parliament and Council of the European Union. "Regulation 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 Council Directive 95/46/EC." Official Journal of the European Union L 119 (2016): 1.
127. Fidler, David P. "Revolt Against or From Within the West?: TWAIL, the Developing World, and the Future Direction of International Law." Articles by Maurer Faculty, 2003.

128. Foo Yun Chee. 2019. “Yet to Show Its Teeth, Landmark EU Privacy Law Already a Global Standard.” Reuters, May 22, 2019. (Alternative listing—merged with “Chee, Foo Yun.”)
129. G Mugano and N Dorasamy, eds. *SMEs and Economic Development in Africa*. 1st ed. Routledge, 2023.
130. Gabon, Law No 001/2011 Relating to the Protection of Personal Data.
131. Gandhi, Dhruv. 2018. “Figure of the Week: Africa’s New Trading Partners.” Brookings, March 7, 2018.
132. Garrett A. Johnson. “Economic Research on Privacy Regulation: Lessons from the GDPR and Beyond.” Questrom School of Business, Boston University (16 June 2023).
133. Gavison, Ruth. “Privacy and the Limits of Law.” (1980) 89:3 *The Yale Law Journal* 421–471.
134. Gordon Woodman. “Legal Pluralism in Africa: The Implications of State Recognition of Customary Laws Illustrated from the Field of Land Law.” (2011) 35 *Acta Juridica*.
135. Greenleaf, G. “African Data Privacy Laws: Implications of Legal and Economic Disparities.” (2019) *Privacy Laws & Business Int’l Rep* 158: 30–35.
136. Greenleaf, G. “Global Data Privacy Laws 2019: 132 National Laws & Many Bills.” (2019) *Privacy Laws & Business Int’l Rep* 158: 22–30.
137. Greenleaf, Graham & Bertil Cottier. “Comparing African Data Privacy Laws: International, African and Regional Commitments.” University of New South Wales Law Research Series 26 (2020).
138. Greenleaf, Graham & Bertil Cottier. “International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis.” *Computer Law & Security Review* 44 (2022): 105638.

139. Greenleaf, Graham. ““Modernised’ Data Protection Convention 108 and the GDPR.” *Privacy Laws & Business International Report*, no. 154 (2018): 22–23, [2019] UNSWLRS 3.
140. Gutwirth, S. *Privacy and the Information Age*. Lanham/Boulder/New York/Oxford: Rowman & Littlefield Publishers, Inc., 2002 at 24–29.
141. Halydier, G. “A Hybrid Legal and Economic Development Model that Balances Intellectual Property Protection and Economic Growth: A Case Study of India, Brazil, Indonesia, and Vietnam.” (2012) 14:1 *Asian-Pac L & Policy J* 87.
142. Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA).
143. Herbert J. Foster. “African Patterns in the Afro-American Family.” (1983) 14 *J Black Stud* 210.
144. Hlomani, Hanani, and Caroline B. Ncube. “Data Regulation in Africa: Free Flow of Data, Open Data Regimes and Cybersecurity.” In *Data Governance and Policy in Africa*, edited by Bitange Ndemo, Njuguna Ndung’u, Scholastica Odhiambo, and Abebe Shimeles, 97–130. Cham, Switzerland: Palgrave Macmillan, 2023.
145. Hogan Lovells. 2023. “Recent Developments in African Data Protection Laws – Outlook for 2023.” *Lexology*, February 24, 2023.
146. Honig, L. “Traditional Leaders and Development in Africa.” (2019) *Oxford Research Encyclopedia of Politics*.
147. Hunter. “Global Justice and Regional Metaphysics. On the Critical History of the Law of Nature and Nations.” In *Law and Politics in British Colonial Thought: Transpositions of Empire*, edited by S. Dorsett and I. Hunter, 13–20. Basingstoke: Palgrave Macmillan, 2010.
148. Ikuenobe, Polycarp. 2006. *Philosophical Perspectives on Communalism and Morality in African Traditions*. Lanham: Lexington Books.

149. International Covenant on Civil and Political Rights (ICCPR). Adopted 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976).
150. International Trade Centre. Promoting SME Competitiveness in Africa: Data for De-Risking Investment, Geneva, September 2018.
151. Jacques Frémont. “Legal Pluralism, Customary Law and Human Rights in Francophone African Countries.” (2009) *Victoria U. Wellington L. Rev.* 149, 150 et seq.
152. Jake Bright and Aubrey Hruby. “The Rise of Silicon Savannah and Africa’s Tech Movement.” *TechCrunch* (23 July 2015).
153. Joireman, Sandra Fullerton. 2001. “Inherited Legal Systems and Effective Rule of Law: Africa and the Colonial Legacy.” 39 *J. Mod. Afr. Stud.* 571, 576.
154. Josiah A. M. Cobbah. “African Values and the Human Rights Debate: An African Perspective.” *Human Rights Quarterly* 9, no. 3 (August 1987): 309–331.
155. Justin Bryant. “Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights.” *Stanford Technology Law Review* 24, no. 2 (2021): 389–446.
156. Kenya Law. 2019. Data Protection Act, 2019.
157. Kenya, The Data Protection Act, No 24 of 2019.
158. Kenya Institute for Public Policy Research and Analysis (KIPPRA). “Strengthening Data Protection in Kenya: Opportunities and the Way Forward” (30 March 2022). <https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/>
159. Kiggundu, J. “Giving Teeth to the African Union: Advancing Compliance with Data Privacy Norms.” (2021) 45–65.

160. Koskeniemi, Martti. "Histories of International Law: Dealing with Eurocentrism." *Rechtsgeschichte – Legal History* 19 (2011): 152–176.
161. Kusamotu, A. "Privacy Law and Technology in Nigeria: The Legal Framework Will Not Meet the Test of Adequacy as Mandated by Article 25 of European Union Directive 95/46." *Information & Communications Technology Law* 16, no. 2 (2007): 149–159.
162. Kwet, M. 2019. "Digital Colonialism: US Empire and the New Imperialism in the Global South." *Race & Class* 60(4), 3–26.
163. Law No. 010-2004/AN on the Protection of Personal Data. Adopted 20 April 2004, Burkina Faso.
164. Law No. 058/2021 on the Protection of Personal Data and Privacy. Rwanda.
165. Law No. 1/2011 on Personal Data Protection. Gabon.
166. Law No. 133-V-2001 on the Protection of Personal Data. Enacted 22 January 2001, Cape Verde.
167. Law No. 2008-12 on the Protection of Personal Data. Enacted 25 January 2008, Senegal.
168. Law No. 2009-09 on the Protection of Personal Data. Adopted 22 May 2009, Benin.
169. Law No. 2013-015 on the Protection of Personal Data. 21 May 2013, Mali.
170. Law No. 2014-038 on the Protection of Personal Data. Republic of Madagascar.
171. Law No. 2017-28 on the Protection of Personal Data. 3 May 2017, Niger.
172. Law No. 2019-014 on the Protection of Personal Data. Enacted on 29 October 2019, Togo.
173. Law No. 22/11 on the Protection of Personal Data. Enacted on 17 June 2011, Angola.
174. Law No. 2017-020 on the Protection of Personal Data. Mauritania.

175. Law No. 2019-71 of 24 December 2019. Creates the High Authority for the Protection of Personal Data (HAPDP), Niger.
176. Law No. 29-2019 on the Protection of Personal Data. Republic of Congo.
177. Lawyers Hub. Africa Privacy Report 2023/2024: A Review of Policy Trends and Digital Frontiers in Africa's Data Protection Landscape (2023), Nairobi, Kenya: Lawyers Hub.
178. Lucima, O. "Reconciliation and Justice: 'Mato Oput' and the Amnesty Act 2002." (2010).
<https://www.c-r.org/accord/northern-uganda/reconciliation-and-justice-%E2%80%98mato-oput%E2%80%99-and-amnesty-act-2002>
179. M L Jones and M E Kaminski. "An American's Guide to the GDPR." *Denver Law Review* 98(1) (2020): 93.
180. Maasai Wilderness Conservation Trust. Equator Initiative Case Study (2013), UNDP.
181. Makulilo, A B. "Privacy Values in African Societies." (2016) 8:2 *Journal of Privacy Studies* 193 at 195.
182. Makulilo, A.B. "A Person Is a Person through Other Persons—A Critical Analysis of Privacy and Culture in Africa." (2016) 7 *Beijing Law Review* 192–204.
183. Makulilo, A.B. "African Data Privacy Laws." In *African Data Privacy Laws*, edited by Alex B. Makulilo, 371–377 (2016).
184. Makulilo, A.B. "'One Size Fits All': Does Europe Impose Its Data Protection Regime on Africa?" *Datenschutz und Datensicherheit* 37, no. 447 (2013): 450.
185. Makau Mutua & Antony Anghie. 2000. "What Is TWAIL?" 94 *Cambridge University Press on Behalf of the American Society of International Law* 31–40.

186. Mamba, AJ. *ICT Law Book: A Source Book for Information and Communication Technologies & Cyber Law in Tanzania & East African Community*. African Books Collective, 2010.
187. Manda, MI & Backhouse, J. “Addressing Trust, Security and Privacy Concerns in E-Government Integration, Interoperability and Information Sharing Through Policy: A Case of South Africa.”
188. Manu J Sebastian. “The European Union’s General Data Protection Regulation: How Will It Affect Non-Enterprises?” *Syracuse Journal of Science and Technology Law* 31 (2015): 216–218.
189. Mark Scott and Laurens Cerulus. “Europe’s New Data Protection Rules Export Privacy Standards Worldwide.” *Politico* (31 January 2018).
190. Masoud, Tarek, Jason Brownlee, and Andrew Reynolds. *The Arab Spring: Pathways of Repression and Reform*. Oxford University Press, 2015.
191. Mastercard Newsroom. “Small and Medium Enterprises Are Big Business.” (25 May 2023).
192. Menkiti, Ifeanyi A. 1984. “Person and Community in African Traditional Thought.” In *African Philosophy: An Introduction*, edited by Richard A. Wright, 171–81. New York: University Press of America.
193. Molefe, Motsamai. “Individualism in African Moral Cultures.” *Cultura: International Journal of Philosophy of Culture and Axiology* 14, no. 2 (2017): 49–68.
194. Mumbere, Daniel. 2019. “Digital in 2018: Africa’s Internet Users Increase by 20%.” *Africanews*. Updated December 9, 2019.
195. Mutua, Makau wa. “Savages, Victims, and Saviors: The Metaphor of Human Rights.” *Harvard International Law Journal* 42 (2001): 201–234.

196. Naidoo, J. "Namibia's Community-Based Natural Resource Management Program: The Politics of Communal Land Tenure and the Management of Local Natural Resources." (2011).
197. Ncube, C. "A Comparative Analysis of Zimbabwean and South African Data Protection Systems." *Journal of Information, Law & Technology* 2 (2004): 18.
198. Ncube, CB. "Data Protection in Zimbabwe." In *African Data Privacy Laws*, 2016, 99–116.
199. Ndemo, Bitange, Njuguna Ndung'u, Scholastica Odhiambo, and Abebe Shimeles, eds. *Data Governance and Policy in Africa*. Springer International Publishing, 2023.
200. Ndeunyema, Ndjodi. "The Namibian Constitution, International Law and the Courts: A Critique." *Global Journal of Comparative Law* (2020): at. 4.1, 271ss.
201. Neethling, J. *Die Reg op Privaatheid* (LLD Thesis, University of South Africa, 1976).
202. Niara Sudarkasa. "African and Afro-American Family Structure: A Comparison." *Black Scholar* 11 (November/December 1980): 44.
203. Nigeria Data Protection Regulation. 2019.
204. Nnaemeka, Johnkingsley. 2023. "A Critical Discourse on African Communalism Vis-a-Vis Western Individualism: The Existential Realities." *SSRN Electronic Journal*.
205. Nyerere, Julius K. "South-South Option." In *The Third World Strategy: Economic and Political Cohesion in the South*, edited by Altaf Gauhar, 9–10. 1983.
206. O'Donoghue, Cynthia. 2013. "Francophone Data Protection Authorities Postpone Adoption of a New Framework for International Data Transfers." *Tech. Law Dispatch*, March 29, 2013.
207. Ochuba, N. A. et al. "Innovations in Business Models through Strategic Analytics and Management: Conceptual Exploration for Sustainable Growth." (2024) 6:3 *Int'l J Mgmt & Ent Res* 554–566.

208. Oguamanam, C. “Indigenous Peoples, Data Sovereignty, and Self-Determination: Current Realities and Imperatives.” (2020) 26 Afr J Info & Comm 1–20.
209. Okafor, Obiora Chinedu. “Critical Third World Approaches to International Law (TWAIL): Theory, Methodology, or Both?” *International Community Law Review* 10 (2008): 371–378.
210. Okafor, Obiora Chinedu. “Newness, Imperialism, and International Legal Reform in Our Time: A TWAIL Perspective.” *Osgoode Hall Law Journal* 43 (2005): 171.
211. Olinger, Hanno N., Johannes J. Britz & Martin S. Olivier. “Western Privacy and/or Ubuntu? Some Critical Comments on the Influences in the Forthcoming Data Privacy Bill in South Africa.” (2007) 39:1 *The International Information & Library Review* 31–43.
212. OneTrust DataGuidance. “Comparing Privacy Laws: GDPR v. POPIA.” (No date provided.)
213. Paradigm Initiative and Olumide Babalola LP. *Data Protection Authorities in Africa: A Report on the Establishment, Independence, Impartiality and Efficiency of Data Protection Supervisory Authorities in the Two Decades of their Existence on the Continent* (July 2021). Lagos, Nigeria: Paradigm Initiative.
214. People’s Republic of Zanzibar Constitution (1984).
215. Policy and Regulatory Initiative for Digital Africa (PRIDA). Launched by the African Union, the European Union, and the International Telecommunication Union, initiated in 2018.
216. Pourmokhtari, N. “A Postcolonial Critique of State Sovereignty in IR: The Contradictory Legacy of a ‘West-centric’ Discipline.” (2013) 34:10 *Third World Q* 1767–1793.
217. Protection of Personal Information Act, 2013 (Act No. 4 of 2013). South Africa.

218. Protocol Amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+). Council of Europe, opened for signature 10 October 2018, CETS No. 223.
219. PwC. “A Privacy Reset — From Compliance to Trust-Building.” PwC (2024).
220. R Li. “South African Government Fined for Data Breach.” ALB (2023).
221. 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 (General Data Protection Regulation). [2016] OJ L 119/1, art 45.
222. Reid, Richard. “How Colonialism Preempted Modernity in Africa.” (2011) 39:3 *The Journal of Imperial and Commonwealth History* 536–538.
223. Republic of Congo, Law No 29-2019 on the Protection of Personal Data.
224. Resolution on the Right to Freedom of Information and Expression on the Internet in Africa. ACHPR/Res. 362(LIX) 2016.
225. Rule of Law Index, WORLD BANK. Archived (12 November 2019).
226. S Sheik. “Data Protection Fines in Africa.” Michalsons.com (2023).
227. Sabina Frizell. “How Kenya’s New Data Privacy Bill Could Hurt Its Economy.” Council on Foreign Relations (8 November 2018).
228. SADC Model Law on Data Protection. Southern African Development Community, adopted 2013.
229. Scott, Mark, and Laurens Cerulus. “Europe’s New Data Protection Rules Export Privacy Standards Worldwide.” Politico, January 31, 2018.
230. SecurityScorecard. “Countries With GDPR-Like Data Privacy Laws.” (No date provided.)
231. Senegal, Law No. 2008-12 of 25 January 2008 on the Protection of Personal Data.

232. Sia Partners. “Survey on GDPR Compliance Costs by Industry.” Sia Partners (May 2018).
233. Solove, D. J. “Privacy Self-Management and the Consent Dilemma.” (2013) 126 Harv L Rev 1880.
234. Solove, D. “The Three General Approaches to Privacy Regulation.” Teach Privacy (2020).
235. Somalia, Constitution (Provisional Constitution, 2012).
236. South African Law Reform Commission. Privacy and Data Protection Project 124 (Project Leader: J Neethling, 2001).
237. Southern Africa Development Community (SADC). Established by the Treaty of Windhoek, 17 August 1992.

Southern African Development Community. 2009. “Model Law on Data Protection.”
238. Summary: Fur, eHRAF World Cultures.
239. Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS. Adopted 16 February 2010.
240. São Tomé and Príncipe, Law No 03/2016 on the Protection of Personal Data.
241. Thomson Reuters. “Top Five Concerns for GDPR Compliance.” (No date provided.)
242. Timileyin Oluwatobi. “Unveiling the Tapestry: Exploring the Intersections of Culture and Society.” Medium. (No date given.)
243. Togo, Law No. 2019-014 Relating to the Protection of Personal Data.
244. Traça, João Luís & Bernardo Emrby. 2011. “An Overview of the Legal Regime for Data Protection in Cape Verde.” 1 Int’l Data Priv. L. 249, 251.
245. Tunisia, Organic Act No 2004-63 of 27 July 2004 on the Protection of Personal Data.
246. Tzouvala, Ntina. “The Specter of Eurocentrism in International Legal History.” Yale Journal of Law & the Humanities 31, no. 2 (2021): 413–433.

247. Udoh, Victoria & David Ademola Olajide. 2021. "Data Protection in Nigeria: A Review of the Nigerian Data Protection Regulation 2019 and the Need for Nigeria to Sign the African Convention on Data Protection." SSRN Electronic Journal.
248. Uganda, The Data Protection and Privacy Act, 2019.
249. Ukwendu, Jeanne Egbosiuba. "AFRICAN PROVERBS ON PREGNANCY AND BIRTH." Bella Online, The Voice of Women.
250. United Nations Conference on Trade and Development (UNCTAD). "The African Continental Free Trade Area: The Day After the Kigali Summit." Policy Brief No. 67 (May 2018).
251. Universal Declaration of Human Rights (UDHR). Adopted by the General Assembly on 10 December 1948, GA Res 217A (III), UN Doc A/810 at 71 (1948).
252. Uwe Kischel and Andrew Hammel. "The Context of African Law." In Comparative Law (Oxford, 2019; online edn, Oxford Academic, 17 April 2019).
253. VAN DER WALT, B.J. 1997. "Afrocentric or Eurocentric: Our Task in Multicultural South Africa." Potchefstroom University for CHE.
254. Warren, Samuel D. & Louis D. Brandeis. "The Right to Privacy." (1890) 4:5 Harvard Law Review 193–220.
255. Westin, Alan F. "Privacy and Freedom." (1968) 25 Wash. & Lee L. Rev. 166.
256. Whitman, James Q. "The Two Western Cultures of Privacy: Dignity Versus Liberty." (No journal/year provided.)
257. Wiessner, S. "The Cultural Rights of Indigenous Peoples: Achievements and Continuing Challenges." (2011) 22:1 Eur J Int'l L 121–140.
258. Zimu-Biyela, Acquinnatta N. "Taking Stock of Oral History Archives in a Village in KwaZulu-Natal Province, South Africa: Are Preservation and Publishing Feasible?" SciELO.