University of Dar es Salaam Library Journal
Vol 18, No 2 (2023), pp 36-53
ISSN: 0856-1818

Africa's Data Privacy Puzzle: Data Privacy Laws and Compliance in Selected African Countries

Sarah Kaddu
College of Computing and Information Sciences, Makerere University
Email: sarah.kaddu@mak.ac.ug

Francis Ssekitto
College of Computing and Information Sciences, Makerere University
Email: francisssekitto@gmail.com

Abstract

This study sought to give a thorough analysis of data privacy legislation, compliance rates, enforcement strategies, and related issues in seventeen (17) African countries that were chosen for the study. The study's objectives were to assess the state of data privacy laws in selected African countries, analyse levels of compliance among entities operating within these countries, assess the effectiveness of enforcement mechanisms, and identify and analyse the common challenges African countries face in complying with and enforcing data privacy laws. Researchers conducted a systematic review of 48 data privacy publications to gain a deep understanding of the complex data privacy landscape. This involved rigorous criteria for inclusion/exclusion, comprehensive search strategies, quality assessment, and data extraction/synthesis. While 15 African countries have implemented comprehensive data privacy legislation, two (Ethiopia and Burundi) rely on general regulations. The analysis found that regulatory bodies significantly enhance compliance, and highlighted recurring challenges such as insufficient public awareness, resource limitations, and complex governance structures. The research underscores the crucial role of dedicated legislation, public education, empowered regulatory authorities, and regional collaboration in guaranteeing data privacy rights in the digital age across Africa.

Keywords: Data Privacy; compliance; enforcement; data Protection laws; Africa
https://dx.doi.org/10.4314/udslj.v18i2.4

Background

The concept of privacy has been around for millennia. For example, this concept was embedded in ancient Egyptian civilisation, visible in housing, religious and spiritual beliefs, social structure, dressing and modesty, and hierographic stelae (Akintola, 2018; Sigerist, 2018; Wengrow, 2018). These aspects indicate some sort of privacy found in various African ways of life. While ancient African societies may not have had the same concept of privacy as we do in the modern world, they likely had some understanding of personal boundaries and modesty. However, their emphasis on communal living, close-knit family structures, and religious practices may have limited the degree of privacy in their daily lives compared with contemporary Western societies. Makulilo (2016a, p. 3) observes that "*since the 1950s and 1960s when the computer was invented to date, privacy has been regarded as a preserve of Western societies partly because outside the Western hemisphere there has been little or no preoccupation in the privacy field*". However, the ubiquity of the internet and the rapid proliferation of technology have given rise to a data-driven landscape in which the protection

of individual privacy is of increasing concern (Abebe *et al.*, 2021; Aydin *et al.*, 2020; Conrad, 2022).

There has been an inclusive debate about how cultures outside the Western world handle the idea of privacy, both in their everyday lives and in their laws. Wambiri *et al.,* (2023) in the context of African countries, the right to privacy hasn't been well defined, explained, or protected. Moreover, several African societies view privacy in the context of collectivism, communism, and interdependence (Bidwell, 2023; Prinsloo & Kaliisa, 2022; Makulilo, 2016), rather than individualism, meaning that concerns about personal privacy are not as prevalent because culture places greater importance on the interests of the group as a whole, as opposed to individual interests. Notwithstanding, several scholars still note that privacy is very difficult or impossible to define, and its conceptualisation appears to be narrow (Oukemeni *et al.*, 2019; Prinsloo & Kaliisa, 2022,; Ukwueze, 2021).

In the context of this study, privacy is the ability of an individual or group to keep its personal information and activities away from public scrutiny or unauthorised access (Ekweozor, 2020; Sikhuphela *et al.*, 2018). Suffice it to note, that there is a complexity of the relationship between privacy that encompasses various aspects like bodily privacy and territorial privacy, and information privacy (data protection) focusing on safeguarding 'personal data.' Makulilo (2016a) and Aydin *et at.,* (2020) elucidate that, while they are related, they have distinct characteristics and legal frameworks, such as the General Data Protection Regulation, 2016. In essence, data privacy is considered a subset of general privacy, concentrating on the protection of personal information amidst the broader spectrum of privacy concerns in African countries today. To ensure consistency, the study maintains the term data privacy and protection to refer to privacy context as leveraged in studies of Katugugu (2019); Makulilo (2016a) and Prinsloo and Kaliisa (2022).

The digital revolution in Africa has brought with it both opportunities and challenges. While there have also been chances for economic growth, innovation, and connectedness, there have been new challenges on the security and privacy of personal information (Ball, 2017; Toapanta *et al.*, 2019). Recognising these dynamics, many African nations have enacted data privacy laws and regulations to safeguard the rights and interests of their citizens. This article compares and contrasts the laws, philosophies, and compliance levels of several African nations as it examines their data privacy environments in great detail. It seeks to shed light on how data privacy laws are changing around the world, how they are enforced, and how well these laws are followed in each country.

Data privacy concerns are growing globally, with limited research specifically focused on African nations. While studies have explored data privacy policies in 14 African countries, highlighting inconsistencies and low compliance, a comprehensive understanding of data privacy laws and practices across the entire continent remains absent. This knowledge gap hinders informed policymaking and effective decision-making in a critical area for African economic development, innovation, and individual rights. Additionally, a lack of understanding of compliance standards and enforcement strategies exacerbates these challenges. This study aimed at providing a comprehensive examination of data privacy laws, compliance levels, enforcement mechanisms, and associated challenges across seventeen (17) selected African countries. The study was guided by the following objectives; To assess the status of data privacy laws in the selected African countries; To analyse the levels of compliance among entities operating within these countries; To evaluate the effectiveness of enforcement mechanisms, including the role of regulatory bodies, and to identify and analyse the common challenges faced by African countries in complying with and enforcing data privacy laws.

Literature Review

In this section, we explore the related extant prior and contemporary literature on data privacy laws, compliance, enforcement mechanisms, impact, and challenges in African countries.

Genesis and Influence of International Data Privacy Regulations in Africa

The concept of 'data privacy laws' is not indigenous and is relatively newer in Africa than in Europe and other parts of the world (Baloyi & Kotzé, 2018; Makulilo, 2016a). Africa is experiencing a surge in mobile and internet use but faces technological challenges like unauthorized surveillance, cybersecurity threats, and pressure from Western trade relationships.

Notably, international agreements agreements emphasise the need to establish supervisory authorities responsible for enforcing data protection principles (Bryant, 2021; Prinsloo & Kaliisa, 2022). According to Makulilo (2016a, p. 19):

> *The Council of Europe's Convention number 108 concerning the protection of personal data extended its reach to non-European countries, with Mauritius and Senegal being the first from Africa to accede to these critical instruments*.

Furthermore, this expansion of the Council of Europe's data privacy policy saw Morocco and Tunisia acceding from these regulations (Makulilo, 2016b; Slokenberga, 2020; Tassinari, 2021). Consequently, in October 1995, the influential European Union (EU) Data Protection Directive 95/46/EC[i] emerged, which held particular sway in harmonising data protection laws across the European Union. Moreover, Article 25, mandating legal coverage for personal information transferred outside Europe, exerts a substantial influence on privacy law reforms in non-EU countries.

Subsequently, In Africa, on 16 February 2010, the Economic Community of West African States (ECOWAS) signed the Supplementary Act on Personal Data Protection within ECOWAS (2010)[ii] and Data Protection Model Law for Southern African Development Community (SADC) (Greenleaf, 2019b; Makulilo, 2016a), Additionally, in the same year the East African Community (EAC) adopted the EAC Legal Framework for Cyber Laws. Inclusively, in 2013, French-speaking states signed the Francophone Binding Corporate Rules (BCR) to address the cross-border transfer of personal data among French-speaking countries encompassing those in Africa. In 2014, the African Union (AU) enforced the AU Convention on Cybersecurity and Personal Data Protection[iii] to address cybercrimes, data privacy and protection, electronic transactions and data processing (Ball, 2017). The section concerning data protection, found in Chapter II (Articles 8–23), shares similarities with the EU Directive 95/46/EC. However, the ratification and implementation of this convention have been uneven across member states, and many countries continue to rely on their national legislation (Greenleaf, 2019b).

Comparison of Various Data Privacy Laws in Africa

Across the African continent, the landscape of data privacy laws reveals variations and commonalities among more than 25 countries (Greenleaf, 2019a). For example, Algeria (Law No. 1807 of June 2018) and Angola (Data Protection Law, 2011) have established data protection legislation, with Angola going a step further by creating *Agência de Proteção de Dados* (APD) as its regulatory authority (Makulilo, 2016a; Prinsloo & Kaliisa, 2022; Traça &

Correia, 2016). Similarly, Benin (Digital Code, 2018) shares the establishment of an independent data protection authority with Angola, although it lacks specific online privacy regulations (Greenleaf, 2019a). Moreover, Keakopa and Mosweu (2020) expound that in Botswana (Data Protection Act, 2018), the Information and Data Protection Commission regulates data with stringent transfer regulations, while Burkina Faso (Law No. 001, 2021) boasts a comprehensive data privacy framework but lacks obligations for data protection officers and rules governing cookies and location data (Ouiminga, 2016). Customarily, Cape Verde initiated data privacy laws in 2001 making it the first African country to formulate a comprehensive law, with the *Comissão Nacional de Proteção de Dados Pessoais* overseeing compliance (Makulilo, 2016a; Slokenberga, 2020).

Surprisingly, Chad (Personal Data Protection, 2015), The Democratic Republic of Congo (Law 20/017, 2020), and Egypt (Personal Data Protection Law, 2020) have robust legislation, with Egypt emphasising compliance, enforcement, online privacy, and electronic marketing (Alashry, 2022; Greenleaf & Cottier, 2020, Greenleaf & Cottier,2022). These diverse approaches underscore the evolving data privacy landscape in Africa, with some nations emphasising specific aspects and others developing comprehensive frameworks, despite lingering challenges such as compliance and enforcement, and online privacy regulation gaps discussed below.

Compliance Levels among Entities Concerning Data Privacy Laws in African Countries

According to Manda (2021, p. 311):

> *The lack of a common development agenda often leads to poor compliance, especially in cases where such decisions are not considered a priority, particularly by developing countries that lag in social and economic development.*

It is worth noting that these core reasons contribute to varying and consistently low compliance levels among entities regarding data privacy laws in African countries (Abdulrauf, 2020; Prinsloo & Kaliisa, 2022).

Across the continent, while some businesses and organisations have made substantial efforts to align with data privacy regulations, many others struggle with the implementation of robust compliance measures (Baloyi & Kotzé, 2019). Cases from different African countries highlight this disparity: Higher education institutions in Mozambique, Lesotho, Namibia, Madagascar, and Angola find it difficult to ensure compliance with legislation and regulatory frameworks to ensure student data privacy (Prinsloo & Kaliisa, 2022). In South Africa, despite the presence of the Protection of Personal Information Act (POPIA) 2020, Manda (2021) and Manda and Backhouse (2018) reiterate concerns about the incapability of the government to enforce compliance. In the same way, in Nigeria, despite the existence of the Nigerian Data Protection Regulation (NDPR), compliance challenges persist due to limited awareness, inadequate enforcement mechanisms, and resource constraints (Baloyi & Kotzé, 2019; Kariuki *et al.*, 2020; Nwosu, 2022).

Interestingly, Baloyi and Kotzé (2018, 2019) studies resonate higher levels of compliance in cyber-physical systems and Internet of Things devices (IoT) use in South Africa. Egypt, influenced by the global GDPR framework, is witnessing growing adoption of GDPR standards by entities operating within its borders, especially multinational corporations. However, domestic entities face a more complex compliance landscape due to the lack of a fully aligned national data privacy framework (Alashry, 2022; Dunbar *et al.,* 2021). Additionally, the influence of the European Union's GDPR is evident, with multinational corporations operating in Africa often aligning their data privacy practices with

GDPR standards, setting a benchmark for local entities (Dunbar *et al.,* 2021; Piasecki & Chen, 2022). To raise compliance levels consistently, however, cooperation between governmental agencies, regulatory authorities, and the commercial sector is necessary (Manda, 2021).

Enforcement Mechanisms for Enforcing Data Privacy Laws

Although many countries have taken steps to strengthen their data privacy laws, enforcement mechanisms remain a challenge, particularly in African countries (Yusuf & Adekoya, 2021). Enforcement mechanisms for ensuring compliance with data privacy laws have been the subject of extensive scholarly inquiry. Baloyi and Kotzé (2019) study on guidelines for data privacy compliance highlights one common approach involves regulatory agencies with the authority to investigate and penalise non-compliant organisations. These agencies play a pivotal role in monitoring and enforcing data privacy regulations, as maintained by Bryant, (2021), Greenleaf (2019a) and Neto *et al.,* (2021) in their comprehensive review of enforcement strategies in various African countries such as Nigeria. Additionally, the growing importance of data protection has led to the development of stringent legal frameworks, such as the European Union's General Data Protection Regulation (GDPR), which imposes substantial fines on members or organisations found in breach of data privacy rules (Vorster et al, 2018). Moreover, several scholars argue that private litigation mechanisms are crucial in ensuring compliance, as they empower individuals to seek legal remedies for data breaches (Scholz, 2021). These various mechanisms collectively contribute to a multifaceted approach aimed at safeguarding individuals' privacy rights and promoting adherence to data protection laws.

Challenges in Compliance and Enforcement of Data Privacy Laws

Several challenges confronting African countries in the compliance and enforcement of data privacy laws have shed light on the multifaceted issues that resonate across the continent. Drawing from a synthesis of contemporary and prior literature, Ball (2017) and Bryant (2021) uncover recurring themes that underscore the complexities faced by African nations in safeguarding data privacy rights. One of the foremost challenges lies in the dearth of public awareness and education regarding data privacy issues in Namibia, Zimbabwe Mozambique and Uganda (Makulilo, 2016a; Prinsloo & Kaliisa, 2022). Moreover, Manda's (2021) study on leadership and trust issues as keys to smart governance, emphasises the urgent need for comprehensive awareness campaigns and concerted involvement of African leaders to bridge the knowledge gap and empower individuals and entities to navigate the evolving data privacy landscape effectively. A dissection of Uganda's state on data privacy laws revealed present-day challenges of terrorism, fraud, cyber-attacks, and increasing organised crime and political instabilities (Makulilo, 2016b).

These unwavering hindrances are not confined to Uganda; they prevail entirely in all African states and consistently emerge as significant impediments to robust enforcement mechanisms. Furthermore, it cannot be overstated that governance intricacies loom large, with political stability and commitment to data privacy proving pivotal. As studies by Bryant (2021) and Greenleaf and (Cottier, 2020) have pointed out, countries with stable political environments and unwavering dedication to data privacy exhibit more effective enforcement mechanisms. Collectively, these challenges underscore the intricate nature of data protection issues in Africa and emphasise the need for concerted efforts to address these impediments and strengthen data privacy protection across the continent.

University of Dar es Salaam Library Journal
Vol 18, No 2 (2023), pp 19-35
ISSN: 0856-1818

Methodology

Research Synthesis

This study employed a systematic review, also known as research synthesis methodology, owing to its ability to comprehensively analyse and synthesise existing research and data concerning data privacy and compliance (Canedo *et al.*, 2023; Cheng *et al.*, 2022; Shome *et al.*, 2023). Systematic literature reviews are especially well-suited for ensuring transparency and rigour in comparative analyses of intricate and multifaceted subjects.

Search Process and Source of Data

A systematic search of the literature was the cornerstone of this study, allowing us to define the problem and explore the landscape of data privacy laws and compliance across 17 selected African countries. To facilitate this, we designed a structured research protocol to guide our systematic review process.

Inclusion and Exclusion Process

Within this protocol, the study rigorously implemented the four stages of research synthesis:
(a) Criteria for inclusion and exclusion in the selection of studies: The inclusion of studies was determined by several factors, including their publication date (between 2015 and 2023), their pertinence to the research goals, and the availability of significant information on data privacy and compliance policies in the selected African nations. Dissertations and journalistic writings (blogs), with the exception of those from respectable and competent organisations like the web pages of the African Union and the European Union, were among the studies that were methodically disqualified for not matching these requirements. Throughout this process, 152 sources were initially collected. However, only 48 publications successfully passed through the rigorous inclusion and exclusion criteria, ensuring a focused and relevant dataset for the study.

(b) Search strategies for identifying relevant literature: A systematic search strategy was meticulously developed, encompassing academic databases such as Google Scholar, JSTOR, LawAxiv, Core, digital common repositories, legal repositories, government websites, and resources from international organisations (AU and EU). The strategy employed Boolean operators and a carefully crafted combination of keywords (e.g., “data privacy,” “compliance,” “data protection laws,” “Africa,” and “Sub-Saharan”) to identify relevant literature.

Data Analysis and Presentation

After searching, a great deal of attention was paid to making sure the chosen studies were reliable and of high quality. The study used a standardised quality assessment tool to do this. We were able to assess the studies using this technique according to their methodological soundness, availability of data, and significance to our main research issue. The tables in the next paragraph present the findings from the systematic literature research, which included important conclusions, new trends, and significant differences in data privacy and compliance policies among the various African nations.

Results

This research evaluated the state of data privacy legislation and related policies in 17 African nations by conducting a thorough examination of 48 pertinent publications (Table 4). Notably, it was found that two of these nations—Ethiopia and Burundi—lacked explicit privacy laws covering the protection of personal data. Rather, Ethiopia demonstrated a strong legislative framework, which covered data security and privacy issues. These laws included the Federal Democratic Republic of Ethiopia's 1995 Constitution, the 2005 Criminal Code, the 1960 Civil Code, the Computer Crime Proclamation No. 958/2016, and the Freedom of the Mass Media and Access to Information Proclamation No. 590/2008 (as amended by Media Proclamation No. 1238/2021). As of 2023, Burundi, like some few other countries lacked a dedicated personal data protection law but maintained a collection of laws and regulations related to data protection.

Table 1: Summary of reviewed publications

S/n	Publication Title	Focus/Keywords
1	Abdulrauf, L. A. (2020)	Giving 'teeth' to the African Union to advance compliance with data privacy norms.
2	Abebe, R., Aruleba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S. L., & Sadagopan, S. (2021)	Narratives and counternarratives on data sharing in Africa.
3	African Union Convention on Cyber Security and Personal Data Protection, (2014)	Testimony of AU African Union.
4	Akintola, S. O. (2018)	Legal implications of data sharing in biobanking research in low-income settings: The Nigerian experience.
5	Alashry, M. S. (2022)	Investigating the efficacy of the Egyptian Data Protection Law on Media Freedom: Journalists' Perceptions.
6	Aydin, K., Saglam, R. B., Li, S., & Bulbul, A. (2020)	When GDPR Meets CRAs (Credit Reference Agencies): Looking through the Lens of Twitter.
7	Ball, K. M. (2017)	African Union Convention on Cyber Security and Personal Data Protection.
8	Baloyi, N., & Kotzé, P. (2018)	A data privacy model based on the Internet of Things and cyber-physical systems reference architectures.
9	Baloyi, N., & Kotzé, P. (2019)	Guidelines for data privacy compliance: A focus on cyber-physical systems and the Internet of Things.
10	Bryant, J. (2021)	Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights.
11	Canedo, E. D., Bandeira, I. N., Calazans, A. T. S., Costa, P. H. T., Cançado, E. C. R., & Bonifácio, R. (2023)	Privacy requirements elicitation: A systematic literature review and perception analysis of IT practitioners.
12	Cheng, S., Zhang, J., & Dong, Y. (2022)	How to Understand Data Sensitivity? A Systematic Review by Comparing Four Domains.
13	Conrad, S. S. (2022)	Integrating Data Privacy Principles into Product Design: Teaching "Privacy by Design" to Application Developers and Data Scientists.
14	Directive 95/ /EC of the European Parliament and of the council: Of on the protection of individuals concerning the processing of personal data and on the free movement of such data, 27 Official Journal of the European Communities 83 (1995)	Directive 95/ /EC

15	Dunbar, E., Elizabeth Olsen, H., Salomon, E., Bhatt, S., Mutuku, R., Wasunna, B., Edwards, J., Kolko, B., & Holeman, I. (2021)	Towards Responsible Data Practices in Digital Health: A case study of an open-source community's journey.
16	Supplementary Act A/SA.1/01/10 on personal data protection within ECOWAS, (2010)	Testimony of ECOWAS Economic Community of West African States.
17	Ekweozor, E. (2020)	An Analysis of the Data Privacy and Protection Laws in Nigeria.
18	General Data Protection Regulation, Official Journal of the European Union 261 (2016)	GDPR
19	Greenleaf, G. (2019a)	Global data privacy laws 2019: 132 national laws and many bills.
20	Greenleaf, G. (2019b)	Nigeria Regulates Data Privacy: African and Global Significance.
21	Greenleaf, G., & Cottier, B. (2020)	Comparing African data privacy laws: International, African and regional commitments.
22	Greenleaf, G., & Cottier, B. (2022)	International and regional commitments in African data privacy laws: A comparative analysis.
23	Kariuki, P., Adeleke, J. A., & Ofusori, L. O. (2020)	The role of open data in enabling fiscal transparency and accountability in municipalities in Africa: South Africa and Nigeria case studies.
24	Katugugu, E. (2019)	Legal Alert the Data Protection and Privacy Act is here.
25	Keakopa, T., & Mosweu, O. (2020)	Data protection law in Botswana: opportunities and challenges for records management.
26	Makulilo, A. B. (2016a)	African Data Privacy Laws.
27	Makulilo, A. B. (2016b)	Data Protection in North Africa: Tunisia and Morocco.
28	Manda, M. I. (2021)	Leadership and trust as key pillars in "smart governance" for inclusive growth in the 4th Industrial Revolution (4IR): Evidence from South Africa.
29	Manda, M. I., & Backhouse, J. (2018)	Inclusive digital transformation in South Africa: An institutional perspective.
30	Mfowabo, M., & Vusumuzi, M. (2020)	Educational data mining in higher education in sub-Saharan Africa: A systematic literature review and research agenda.
31	Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021)	Developing a Global Data Breach Database and the Challenges Encountered.
32	Nwosu, C. (2022)	Should One Accept the Cookies? Exploring the Privacy Concerns in Digital Advertising in Nigeria.
33	Ouiminga, K. M. (2016)	Data Protection Law in Burkina Faso.
34	Oukemeni, S., Rifà-Pous, H., & Puig, J. M. M. (2019)	Privacy analysis on microblogging online social networks: A survey.
35	Piasecki, S., & Chen, J. (2022)	Complying with the GDPR when vulnerable people use smart devices.
36	Prinsloo, P., & Kaliisa, R. (2022)	Data privacy on the African continent: Opportunities, challenges and implications for learning analytics.
37	Scholz, L. H. (2021)	Private Rights of Action in Privacy Law.
38	Shome, S., Shankar, A., & Pani, S. K. (2023)	Consumer privacy in smartphones: A systematic literature review.
39	Sikhuphela, A., Gawuza, N., Maka, S., & Jere, N. R. (2018)	Designing technologies for Africa: Does culture matter?
40	Slokenberga, S. (2020)	Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108.
41	Tassinari, F. (2021)	The externalisation of Europe's data protection law in Morocco: an imperative means for the management of migration flows.
42	Toapanta, S. M. T., Gurumendi, A. J., & Gallegos, L. E. M. (2019)	An approach of national and international cybersecurity laws and standards to mitigate information risks in public organisations of Ecuador.

43	Traça, J. L., & Correia, F. (2016)	Data Protection in Angola.
44	Ukwueze, F. O. (2021)	Strengthening the legal framework for personal data protection in Nigeria.
45	Verma, R. M., & Srinivasagopalan, S. (2019)	Clustering for security challenges.
46	Vorster, R., Li, F., Clarke, N., & Furnell, S. (2018)	A comparison of compliance with data privacy requirements in two countries.
47	Wambiri, D., Johnson, M., & Frankline, M. (2023)	Big Data and Personal Information Privacy in Developing Countries: A Case of Kenya.
48	Wengrow, D. (2018)	What makes civilisation? The ancient Near East and the future of the West.

In contrast, the study revealed that the remaining 15 African countries have established comprehensive data privacy laws (see Table 2). These legislative frameworks demonstrated a commitment to enhance data privacy and security, spanning various sectors, including health, agriculture, security, telecommunications, and both the private and public sectors. Despite the commendable progress in the formulation, enforcement, and compliance of data privacy laws, it is important to acknowledge the multifaceted challenges that persist across African countries. These challenges, ranging from governance issues to enforcement complexities, render these nations susceptible to various constraints that affect cross-border transactions, economic markets, and other aspects of their data privacy landscape.

Comparison of Various Data Privacy Laws in Africa

The table below presents findings regarding the comparison of data privacy laws in 17 selected African countries, highlighting both commonalities and differences among the laws.

Table 2: Comparison of various data privacy laws in Africa

Country	Source	Data Privacy Law	Key Provisions
South Africa	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Protection of Personal Information Act (POPIA) (2022)	Defines personal information broadly, encompassing any data that can identify an individual. Mandates explicit consent requirements for data processing. Presence of an Enforcement Committee Grants data subjects' rights, including access, correction, and deletion of their data Requires data breach notifications and imposes fines for non-compliance.
Nigeria	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Nigeria Data Act 2023	Outlines data protection principles, including lawful and fair processing. Grants data subjects have the right to access their data and request corrections. Requires data breach notifications and sanctions for noncompliance.
Kenya	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Data Protection Act, 2019	Emphasises the protection of personal data and imposes obligations on data controllers and processors. Establishes a Data Protection Commissioner and the right to seek legal remedies for data breaches.
Ghana	https://www.data	Data Protection Act, 2012	Defines personal data and data subject rights, similar to

	guidance.com/ https://www.dlapiperdataprotection.com/		other laws. Requires registration with the Data Protection Commission and notification of data breaches.
Egypt	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Personal Data Protection Law, 2020	Defines personal data and data subject rights, aligning with global data protection standards. Requires consent for data processing and establishes the Personal Data Protection Authority. Imposes fines and penalties for noncompliance and data breaches.
Algeria	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Law No. 18-07, 2018 on the protection of natural persons in personal data processing	The law regulates data on ethnicity, religion philosophical beliefs etc. Unestablished National Data Protection Authority Enforcement not by the Authority
Benin	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Law No. 2017-20 and 2018 on digital code Law No. 2009-09 on the protection of Personally Identifiable Information	Similar to other laws The Beninese data protection authority is the regulator and enforcer. DPO as enforcers Electronic marketing No online privacy
Ethiopia	https://www.dlapiperdataprotection.com/	N/A	N/A
Gabon	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Law No. 001/2011 (Protection of Personal Data)	Gabonese National Authority – regulator DPO – exclusive discretion of the data controller No enforcement decisions Electronic Marketing regulated Online data privacy is not protected Law not comprehensive
Republic of Congo	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	The Protection of Personal Data Law, 2019	No Authority (regulator) No -provisions to appoint DPO No enforcement – (No regulator) Electronic Marketing – Separate laws Online privacy – separate laws Law not comprehensive
Chad	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Personal Data Protect, 2015	Agence Nationale de Sécurité Informatique et de Certification Électronique -National Data Protection Authority No – provisions to appoint DPO ANSICE – has powers to enforce Electronic marketing regulated Online privacy is not specified. Law not comprehensive
Morocco	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Privacy and Data Protection, 2009	Agence Nationale de Sécurité Informatique et de Certification Électronique – Regulator No requirements for DPO The commission enforces compliance. Electronic marketing regulated Online privacy regulated The law is comprehensive

Cape Verde	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Data Protection Law 2001	Comissão Nacional de Proteção de Dados Pessoais – the regulator (CNPD) Appointment of DPO is mandatory Enforcement is done by CNPD Electronic Marketing regulated Online privacy regulated Law is comprehensive
Burundi	https://www.dlapiperdataprotection.com/	No data privacy and Protection law	N/A
Burkina Faso	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Law No. 001-2021 of March 30, 2021, on the protection of persons about the processing of personal data. Law 010-2004/AN on the protection of personal data.	Commission de l'Informatique et des Libertés – Regulator No obligation to appoint – DPO CIL is the enforcer of compliance Electronic marketing regulated Online privacy not specified Law is comprehensive
Angola	https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Data protection law, 2011	Agência de Proteção de Dados (APD) – Regulator No requirement to appoint a DPO APD – Enforces for compliance Electronic Marketing specified/regulated Online privacy is regulated and protected Law is comprehensive
Uganda	https://ulii.org/ https://www.dataguidance.com/ https://www.dlapiperdataprotection.com/	Data Privacy and Protection Act, 2019	The office operates under the National Information Technology Authority- Uganda (NITA-U) Requirements for appointing DPO specified NITA-U (data privacy office) enforces for compliance No Electronic Marketing Regulations No Online privacy regulation Law not comprehensive

Compliance Levels among Entities Concerning Data Privacy Laws in Africa

As noted above Again, some countries like Ethiopia and Burundi, lack specific data privacy laws, but instead rely on various related regulations, leading to compliance challenges for entities operating within their borders. Conversely, the other 15 countries established regulatory bodies dedicated to enforcing compliance, resulting in a more structured and steadily progressing compliance landscape.

Table 3: Compliance levels among entities concerning data privacy laws in Africa

Country	Type of Entity	Key Observations
South Africa	Private Sector	Private companies in South Africa generally demonstrate a strong commitment to data privacy compliance.
	Public Sector	Government agencies in South Africa have made progress in implementing data privacy measures, but challenges persist.
Nigeria	Private Sector	Nigerian businesses display varying degrees of awareness and implementation of data privacy practices.

	Healthcare	Healthcare institutions prioritise data privacy but face challenges in ensuring consistent compliance.
Kenya	Private Sector All sectors	Kenyan businesses show willingness to comply with data privacy laws, but enforcement remains a challenge.
	Education	Educational institutions struggle with resource limitations, affecting their ability to fully comply with regulations.
Ghana	Public Sector All sector	Government entities in Ghana have shown improvement in data privacy compliance, particularly in recent years.
	Financial Sector	Financial institutions in Ghana are generally proactive in implementing data privacy measures due to regulatory scrutiny.
Egypt	Private Sector All sectors	Egyptian businesses are in the process of adapting to data privacy requirements, with varying levels of compliance.
	Telecommunication	Telecommunication companies in Egypt have made significant strides in data privacy compliance, given industry regulations.
Algeria	Private Sector Oil Public	In progress, aligning with data privacy laws.
Benin	Private Sector Oil Industry Agriculture	Gradually improving compliance with regulations.
Ethiopia	N/A	N/A
Gabon	Private Sector, Forestry, mining	Actively aligning with data privacy regulations.
Republic of Congo	Mining, Private Sector, Public	Efforts underway, awaiting detailed regulations.
Chad	Private Sector, Education; Health	Adapting to requirements, making compliance progress.
Morocco	Private Sector, Fishing, Health, etc	Actively working towards data privacy compliance.
Cape Verde	Private Sector, All entities	Addressing data privacy compliance.
Burundi	N/A	N/A
Burkina Faso	Private Sector, public and mining	Working to enhance compliance with regulations.
Uganda	Public, private sector	Actively working towards data privacy compliance.

Enforcement Mechanisms for Enforcing Data Privacy Laws

A study found that 15 out of 17 African countries have dedicated regulatory bodies responsible for data privacy enforcement, while the remaining 2 have related bodies with unclear mandates. This highlights the importance of dedicated bodies for effective data privacy enforcement across Africa (See Table 4).

Table 4: Enforcement Mechanisms for enforcing data privacy laws

Country	Regulatory Authority or Body	Key Enforcement Mechanisms and Literature Findings
South Africa	Information Regulator of South Africa (IR)	The Information Regulator in South Africa oversees compliance and enforcement of data privacy laws. The IR conducts investigations, issues compliance notices, and can impose fines for noncompliance. Collaborates with other regulatory bodies and law

		enforcement agencies to ensure data privacy enforcement.
Nigeria	National Information Technology Development Agency (NITDA) Data Protection Commission (DPC)	NITDA is responsible for enforcing data privacy regulations in Nigeria. Can issue sanctions and penalties for noncompliance, including fines and data breach notifications.
Kenya	Data Protection Commission, Ghana	The Data Protection Commissioner has authority over data privacy enforcement in Kenya. Conducts assessments and investigations, issues enforcement notices, and ensures data subjects' rights are upheld. Collaborates with other government agencies to enforce data privacy laws and protect individual rights.
Ghana	National Telecommunication Regulatory Authority (NTRA)	DPC serves as the regulatory body responsible for enforcing data privacy laws in Ghana. Conducts compliance assessments, investigations, and audits to ensure adherence to data protection regulations. Issues enforcement orders, undertakes advocacy and awareness programs, and collaborates with law enforcement agencies.
Egypt	Commission Nationale de l'Informatique et des Libertés (CNIL)	The Personal Data Protection Authority in Egypt is tasked with enforcing data privacy regulations. Can impose fines, revoke licenses, and recommend legal action for severe data privacy violations.
Algeria	Autorité de Régulation des Communications Electroniques et de la Poste (ARCEP)	Regulatory agencies and fines for non-compliance.
Benin	Information Network Security Agency (INSA)	Fines and legal actions against violators.
Ethiopia	Agence de Régulation des Communications Electroniques et de la Poste (ARCEP)	Regulatory authorities not established. Several hindrances due to the absence of law
Gabon	Agence de Régulation des Postes et des Communications Electroniques (ARPCE)	Government agencies enforce data privacy laws.
Republic of Congo	Autorité de Régulation des Communications Electroniques et des Postes (ARCEP)	Enforcement agencies, pending detailed regulations.
Chad	Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP)	Legal actions and penalties for non-compliance.
Morocco	Agência Nacional das Comunicações (ANAC)	Regulatory bodies and penalties for violations.
Cape Verde	Autorité de Régulation des Communications Electroniques et de la Poste (ARCEP)	Authorities overseeing data privacy law compliance.
Burundi	Autorité de Régulation des Communications Electroniques et des Postes (ARCEP)	Regulatory agencies not enforced or established, therefore faced with vast hinders
Burkina Faso	National Information Technology Authority-Uganda (NITA-U)	Regulatory bodies and enforcement of data privacy laws.
Uganda	Information Regulator of South	The regulatory office is similar to that of Kenya, it is tasked

Africa	with enforcing compliance

Challenges in Compliance and Enforcement of Data Privacy Laws

Drawing from a comprehensive review of over 48 data privacy publications in African countries, this research synthesis highlights the recurring challenges faced in enforcing data privacy laws and regulations. The challenges are listed in Table 5.

Table 5: Challenges in compliance and enforcement of data privacy laws

Country	Challenges
South Africa	Lack of awareness among businesses, and inadequate regulatory resources. Limited enforcement capabilities, and insufficient penalties for non-compliance.
Nigeria	Challenges with cross-border data transfers, and weak enforcement mechanisms.
Kenya	Insufficient legal framework, lack of specialised enforcement agencies.
Ghana	Lack of detailed regulations, and limited enforcement capabilities.
Egypt	Resource constraints for enforcement, low awareness among businesses.
Algeria	Lack of comprehensive data privacy laws, and inadequate penalties.
Benin	Limited resources for enforcement, need for awareness campaigns.
Ethiopia	Lack of robust regulatory framework, and limited technical capabilities.
Gabon	Inadequate legal provisions, and insufficient enforcement mechanisms.
Republic of Congo	Limited enforcement capacity, and lack of public awareness.
Chad	Challenges in implementation, lack of coordination among agencies.
Morocco	Need for stricter penalties, and challenges in cross-border data transfers.
Cape Verde	Limited enforcement capacity, gaps in the regulatory framework.
Burundi	Inadequate resources for enforcement, evolving legal landscape.
Burkina Faso	Limited awareness among businesses needs comprehensive laws.
Uganda	Lack of specialised enforcement agencies, and challenges in data sharing.

Discussion

It is clear from this study's thorough examination of data privacy laws in 17 African nations that the region is marked by a complex interaction between similarities and differences. Many African countries are struggling with the creation and implementation of data privacy laws. Two countries that stand out in particular are Ethiopia and Burundi, which rely on related regulations rather than dedicated data privacy laws. This raises important questions regarding the effectiveness of such regulatory mechanisms. (Bryant, 2021). On the other hand, the remaining fifteen countries have acknowledged the necessity of specific, focused data privacy laws, which is consistent with the prevalent research in the literature that emphasises the necessity of all-encompassing legal frameworks (Makulilo, 2016b, 2016a; Mfowabo & Vusumuzi, 2020).

Moreover, an examination of the degree of compliance across the entities in these African countries reveals a clear division. Regulatory commissions or authorities are essential in monitoring and enforcing compliance in nations with specific data privacy laws, promoting a systematic and gradually complying environment. These results add to the body of previous study rather than being entirely novel. Conversely, nations lacking explicit data privacy legislation encounter difficulties with adhering to regulations due to the lack of a well-defined framework, thereby highlighting the crucial function of regulatory bodies (Akintola, 2018; Ball, 2017; Bryant, 2021; Prinsloo & Kaliisa, 2022; Verma & Srinivasa Gopalan, 2019).

It's important to emphasise how urgently these issues must be addressed to improve data privacy protection in Africa. This means that in nations where there are no existing laws

on data privacy, they must create new ones, invest in public awareness initiatives, and strengthen their regulatory agencies' ability to enforce existing rules. Furthermore, to address the compliance issues faced by multinational organisations and enable cross-border data flows, it is imperative to investigate regional harmonisation of data protection legislation.

Conclusions

Finally, the study's extensive research of data privacy in 17 African countries highlights the complexities of the regulatory landscape. Ethiopia and Burundi rely on related legislation rather than dedicated data privacy laws, while the remaining 15 countries have built full legal frameworks. The presence of regulatory organisations has a substantial impact on compliance levels. Our research also discovered reoccurring issues such as a lack of public awareness and a lack of resources. The study highlights the importance of specialised laws, public awareness campaigns, and regional harmonisation efforts. Despite these limitations, this study adds to our understanding of data privacy in Africa by emphasising the need for appropriate policies and powerful enforcement mechanisms to protect data privacy rights.

Recommendations

The significance of the findings derived from the analysis of 48 publications on data privacy in the Sub-Saharan African region cannot be overstated. These findings align with recommendations reiterated by several authors. Furthermore, this study contributes additional strategies and recommendations to the existing literature, which encompass the following:

a) ***Enhance cross-border collaboration:*** African countries should collaborate to harmonise data privacy regulations for a unified approach and information sharing. While progress exists in regional bodies like ECOWAS, SADC, and EAC, gaps in alignment with international members like Europe remain.

b) ***Strengthen enforcement mechanisms***: African governments must ensure that enforcement mechanisms are robust and capable of holding entities accountable for data privacy violations. This includes establishing dedicated data protection authorities with adequate resources and enforcement powers, this is picked from a vast number of countries with laws whilst absence of independent bodies.

c) ***Monitor Compliance Regularly***: Implement regular audits and assessments of data privacy compliance across various sectors and regions. These assessments should identify gaps and areas of improvement, allowing for targeted interventions.

d) ***Encourage industry self-regulation:*** Encouraging industries and businesses to adopt self-regulatory measures to enhance data privacy and protection. This can include industry-specific codes of conduct and certification programs such as those indicated in South African education and health entities.

e) ***International cooperation***: African countries should actively engage in international dialogues and collaborations on data privacy such as Global Partnership for Sustainable Development of Data, UN Global Pulse, and EU. Moreover, learning from the experiences of other countries that have developed compliance frameworks

and participating in international data protection agreements can contribute to more effective policies and practices.

References

Abdulrauf, L. A. (2020). Giving 'teeth' to the African Union to advance compliance with data privacy norms. *Information & Communications Technology Law*, *30*(2), 87–107. https://doi.org/10.1080/13600834.2021.1849953

Abebe, R., Aruleba, K., Birhane, A., Kingsley, S., Obaido, G., Remy, S. L., & Sadagopan, S. (2021). Narratives and counternarratives on data sharing in Africa. *FAccT 2021 - Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 329–341. https://doi.org/10.1145/3442188.3445897

Adeoti, E. (2023). *A New Era of Data Protection and Privacy; Unveiling Innovations & Identifying Gaps in the Nigeria Data Protection Act of 202*3. http://dx.doi.org/10.2139/ssrn.4520238

African Union Convention on Cyber Security and Personal Data Protection, (2014) (testimony of AU African Union).

Akintola, S. O. (2018). Legal implications of data sharing in biobanking research in low-income settings: The Nigerian experience. *South African Journal of Bioethics and Law*, *11*(1), 15. https://doi.org/10.7196/sajbl.2018.v11i1.00601

Alashry, M. S. (2022). Investigating the efficacy of the Egyptian data protection law on media mreedom: Journalists' perceptions. *Communication and Society*, 35(1), 101–118. https://doi.org/10.15581/003.35.1.101-118

Aydin, K., Saglam, R. B., Li, S., & Bulbul, A. (2020). When GDPR Meets CRAs (Credit Reference Agencies): Looking through the Lens of Twitter. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3433174.3433586

Ball, K. M. (2017). African Union convention on cyber security and personal data protection. *International Legal Materials*, *56*(1), 164–192. https://doi.org/10.1017/ilm.2016.3

Baloyi, N., & Kotzé, P. (2018). A data privacy model based on internet of things and cyber-physical systems reference architectures. *ACM International Conference Proceeding Series*, 258–267. https://doi.org/10.1145/3278681.3278712

Baloyi, N., & Kotzé, P. (2019). Guidelines for data privacy compliance: A focus on cyber-physical systems and internet of things. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3351108.3351143

Bryant, J. (2021). Africa in the information age: challenges, opportunities, and strategies for data protection and digital rights. *Stanford Technology Law Review*, *24*(2), 389–439.

Canedo, E. D., Bandeira, I. N., Calazans, A. T. S., Costa, P. H. T., Cançado, E. C. R., & Bonifácio, R. (2023). Privacy requirements elicitation: a systematic literature review and perception analysis of IT practitioners. *Requirements Engineering*, *28*(2), 177–194.

Cheng, S., Zhang, J., & Dong, Y. (2022). How to Understand Data Sensitivity? A Systematic Review by Comparing Four Domains. *ACM International Conference Proceeding Series*, 13–20. https://doi.org/10.1145/3538950.3538953

Conrad, S. S. (2022). Integrating data privacy principles into product design: Teaching privacy by design to application developers and data scientists. *Journal of Computing Sciences in Colleges.*, *38*(3), 132–142.

DATA, P. O. P. (1995). Directive 95/46/EC of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal L*, 281(23/11), 0031-0050.

Dunbar, E., Elizabeth Olsen, H., Salomon, E., Bhatt, S., Mutuku, R., Wasunna, B., …

Holeman, I. (2021). Towards Responsible Data Practices in Digital Health: A case study of an open source community's journey. In *Conference on Human Factors in Computing Systems - Proceedings. Association for Computing Machiner*y. https://doi.org/10.1145/3411763.3443438

Ekweozor, E. (2020). An Analysis of the Data Privacy and Protection Laws in Nigeria. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3639129

General Data Protection Regulation. (2016). General data protection regulation (gdpr) – official legal text. *general data protection regulation*. https://gdpr-info.eu/[Accessed October 5th 2023] Greenleaf, G. (2019a). Global data privacy laws 2019: 132 national laws and many bills. *SSRN Electronic Journal*, 14–18. https://ssrn.com/abstract=3380794

Greenleaf, G. (2019b). Nigeria regulates data privacy: African and global significance. *Privacy Laws & Business International Report*, 23–25.

Greenleaf, G., & Cottier, B. (2020). Comparing African data privacy laws: International, African and regional commitments. *SSRN Electronic Journa*l. https://doi.org/10.2139/ssrn.3582478.

Greenleaf, G., & Cottier, B. (2022). International and regional commitments in African data privacy laws: A comparative analysis. *Computer Law & Security Review*, *44*, 105638.

Kariuki, P., Adeleke, J. A., & Ofusori, L. O. (2020, September). The role of open data in enabling fiscal transparency and accountability in municipalities in Africa: South Africa and Nigeria case studies. In *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance* (pp. 410-418). Katugugu, E. (2019). Legal Alert The Data Protection and Privacy Act is here. Retrieved from https://www.pwc.com/ug/en/assets/pdf/legal-alert-data-protection-and-privacy-act.pdf [Accessed October 5th 2023]

Keakopa, T., & Mosweu, O. (2020). Data protection law in Botswana: opportunities and challenges for records management. *ESARBICA Journal*, *39*(1).

Makulilo, A. B. (2016a). *African data privacy laws.* Springer International Publishing.

Makulilo, A. B. (2016b). Data Protection in North Africa: Tunisia and Morocco. *African Data Privacy Laws*, 27–44.

Manda, M. I. (2021). Leadership and trust as key pillars in "smart governance" for inclusive growth in the 4th Industrial Revolution (4IR): Evidence from South Africa. *ACM International Conference Proceeding Series*, 308–315. https://doi.org/10.1145/3494193.3494235

Manda, M. I., & Backhouse, J. (2018). Inclusive digital transformation in South Africa: An institutional perspective. *ACM International Conference Proceeding Series*, 464–470. https://doi.org/10.1145/3209415.3209486

Maphosa, M., & Maphosa, V. (2020, September). Educational data mining in higher education in sub-Saharan Africa: A systematic literature review and research agenda. In *Proceedings of the 2nd International Conference on Intelligent and Innovative Computing Applications* (pp. 1-7).

Neto, N. N., Madnick, S., Paula, A. M. G. D., & Borges, N. M. (2021). Developing a global data breach database and the challenges encountered. *Journal of Data and Information Quality*, *13*(1), 1–33. https://doi.org/10.1145/3439873

Nwosu, C. (2022). Should one accept the cookies? Exploring the privacy concerns in digital advertising in Nigeria. *SSRN Electronic Journal*, 1–13. https://doi.org/10.2139/ssrn.4262747

Ouiminga, K. M. (2016). Data protection law in Burkina Faso. *African Data Privacy Laws*, 77–98.

Oukemeni, S., Rifà-Pous, H., & Puig, J. M. M. (2019). Privacy analysis on microblogging online social networks: A survey. *ACM Computing Surveys (CSUR)*, 52(3), 1-36. Piasecki, S., & Chen, J. (2022). Complying with the GDPR when vulnerable people use smart devices. *International Data Privacy Law*, *12*(2), 113–131. https://doi.org/10.1093/idpl/ipac001

Prinsloo, P., & Kaliisa, R. (2022). Data privacy on the African continent: Opportunities, challenges and implications for learning analytics. *British Journal of Educational Technology*, *53*(4), 894–913. https://doi.org/10.1111/bjet.13226

Scholz, L. H. (2021). Private Rights of Action in Privacy Law. *Wm. & Mary L. Rev.*, 63, 1639.

Shome, S., Shankar, A., & Pani, S. K. (2023). Consumer privacy in smartphones: a systematic literature review. *Journal of Consumer Marketing*. (ahead-of-print)

Sigerist, H. E. (2018). *Civilization and disease*. Cornell University Press.

Sikhuphela, A., Gawuza, N., Maka, S., & Jere, N. R. (2018). Designing technologies for Africa: Does culture matter? *ACM International Conference Proceeding Series*, 275–276. https://doi.org/10.1145/3283458.3283504

Slokenberga, S. (2020). Biobanking and data transfer between the EU and Cape Verde, Mauritius, Morocco, Senegal, and Tunisia: adequacy considerations and Convention 108. *International Data Privacy Law*, *10*(2), 132–145.

Tassinari, F. (2021). The externalisation of Europe's data protection law in Morocco: An imperative means for the management of migration flows. *The Externalisation of Europe's Data Protection Law in Morocco: An Imperative Means for the Management of Migration Flows*, 263–282.

Toapanta, S. M. T., Gurumendi, A. J., & Gallegos, L. E. M. (2019, December). An approach of national and international cybersecurity laws and standards to mitigate information risks in public organizations of ecuador. In *Proceedings of the 2019 2nd International Conference on Education Technology Management* (pp. 61-66).Traça, J. L., & Correia, F. (2016). Data Protection in Angola. *African Data Privacy Laws*, 349–362.

Ukwueze, F. (2021). Strengthening the Legal framework for personal data protection in Nigeria. *The Nigerian Juridical Review*, 16, 124-142.

Verma, R. M., & Srinivasagopalan, S. (2019, March). Clustering for security challenges. In *Proceedings of the ACM International Workshop on Security and Privacy Analytics* (pp. 1-2).

Da Veiga, A., Vorster, R., Li, F., Clarke, N., & Furnell, S. (2018, June). A comparison of compliance with data privacy requirements in two countries. *In 26th European Conference on Information Systems.* University of Portsmouth.

Wambiri, D., Johnson, M., & Frankline, M. (2023). *Big Data and Personal Information Privacy in Developing Countries : A Case of Kenya*. 1–10. https://doi.org/10.21203/rs.3.rs-2604181/v1

Wengrow, D. (2018). *What makes civilization?: The ancient near East and the future of the West*. Oxford University Press.

Yusuf, S. K., & Adekoya, O. M. (2021). Trends in Contemporary Record Management. In *Handbook of Research on Information and Records Management in the Fourth Industrial Revolution* (pp. 326-343). IGI Global.