African Journal on Privacy & Data Protection

2025

African Journal on Privacy & Data Protection
https://www.ajpdp.unilag.edu.ng

The financial support of Meta is gratefully acknowledged

African Journal on Privacy & Data Protection

Volume 2 ~ 2025

Pretoria University Law Press
PULP
publishing African scholarship that matters
www.pulp.up.ac.za

2025

African Journal on Privacy and Data Protection

Published by:
Pretoria University Law Press (PULP)
The Pretoria University Law Press (PULP) is a publisher at the Faculty of Law, University of Pretoria, South Africa. PULP endeavours to publish and make available innovative, high-quality scholarly texts on law in Africa. PULP also publishes a series of collections of legal documents related to public law in Africa, as well as text books from African countries other than South Africa. This book was peer reviewed prior to publication.

For more information on PULP, see www.pulp.up.ac.za

Printed and bound by:
Pinetown Printers, South Africa

To order, contact:
PULP
Faculty of Law
University of Pretoria
South Africa
0002
pulp@up.ac.za
www.pulp.up.ac.za

Cover design:
DN Ikpo

ISSN: 3007-8997

African Journal on Privacy & Data Protection

Contents

African Journal on Privacy & Data Protection

Editorial ~ Volume 2, 2025

https://doi.org/10.29053/ajpdp.v2i1.0001

We are excited to present to our audience the second volume of the *African Journal on Privacy and Data Protection*. Building on the gains and achievements of the first volume, the second volume presents six articles that interrogate and reflect on the continuously evolving dimension of privacy and data protection in diverse areas of Africa's evolving digital landscape. Areas interrogated by scholarship in this volume include African data protection enforcement mechanisms; access to information and privacy rights; children's rights to privacy; persons with disabilities; and artificial intelligence algorithm discrimination; and so forth. Just as in the first volume, the jurisdictional scope of the articles in this volume is also truly African and diverse. The volume features scholarship from South Africa, Kenya, Tanzania and Nigeria, among others.

In the face of the exponential increase of Africa's internet users projected to reach 1,1 billion in 2029 and the growing concern of personal data protection in Africa in the era of surveillance capitalism and digital colonialism, Raji and others analysed and evaluated African data protection laws enforcement mechanisms in the first article. By analysing the data protection laws of 20 African countries, the authors identified unique trends, common patterns and best practices that may serve as a guide to inform reform options and practices of critical stakeholders involved in data collection and processing in African countries and ultimately shape future regional policy and data protection laws and practices. The article closes a significant gap existing on the topic that hitherto has been focused on summarising individual countries' data protection frameworks and/or comparing these to the European Union (EU) General Data Protection Regulation.

In the second article Genga makes important arguments about the protection of the rights of persons with disabilities (PWDs) in the era of the proliferation of the use of artificial intelligence (AI). The author observed that although the advent of and widespread use of AI have and continue to enhance the quality of life and participation of PWDs in society, AI algorithm discrimination

concerns have become significant for PWDs because of the uptake of the use of AI in sectors where PWDs have historically encountered and continue to encounter discrimination and exclusion. The author notes that one of the few ways in which AI algorithm discriminations can be engaged is through data protection laws. Consequently, the author interrogated the adequacy of Kenya's and South Africa's data protection frameworks in protecting PWDs from AI algorithm discrimination. The scholar found that although both frameworks attempt to engage the challenge, they did not adequately reflect or implement the transparency and explainability principles in the use of AI and, consequently, are unable to adequately protect the rights of PWDs from AI algorithm discrimination.

Simiyu, in the third article, also uses Kenya and South Africa as case studies. The author interrogates the conflict and potential collision between the rights to privacy and access to information in the current digital age, especially during elections and electioneering processes in Africa. The scholar analysed and assessed the extent to which relevant international, regional and domestic frameworks mediate the conflicts between the two rights in Africa, and notes that the effective implementation of the frameworks and mediation of the potential collision between the two rights rests on enforcement actors of which the judiciary is paramount. The scholar found that while regional frameworks impressively advance access to information, there are gaps with regard to the protection of the corresponding rights of privacy and data protection. Simiyu underscores the importance of a holistic reading of international, regional and domestic frameworks in balancing the conflicts between the two rights, and concludes that both South Africa's and Kenya's frameworks and courts fare much better in the balancing and mediation of the potential collision between the two rights.

In the fourth article Babalola takes an excursion into history and interrogates the origin of the right to privacy in Nigeria's constitutional regime. Although there is some literature that attempts to trace the origin of the right in Nigeria's constitutional frameworks, there are inconsistencies in the academic accounts. Through a review of relevant case law and authoritative constitutional documents, Babalola traces the constitutional origin of privacy in Nigeria to the Schedule of the 1954 (Lyttleton) Constitution. The article arguably puts the controversy regarding the origin of privacy in Nigeria to rest and highlights the influence of the European Convention on Human Rights on Nigeria's constitutional rights development.

The last two articles underscore the growing importance of African children's rights to privacy and online protection in the current digital age. In their article, Joseph and Mwakisiki set the proper foundation for this discussion within the context of the continuous evolution of Africa's digital landscape. The authors conduct a comprehensive review of international and regional frameworks for the protection of the right to privacy and protection of personal data of children.

They thereafter undertake a critical assessment of Tanzania's domestic frameworks. They identified several loopholes and exceptions that can be exploited by perpetrators to violate children's rights to privacy and safety in cyberspace. The authors also highlighted the vital roles of the courts in bridging the ever-present and widening gaps between the development of the law and technology towards more effective protection of children's rights to privacy and safety in cyberspace.

Finally, Arowolo in her article conducts an extensive review of international, regional and comparative foreign law frameworks for the protection of the privacy, data protection and safety of children online. In light of the frameworks reviewed, Arowolo assesses the extent to which children's rights to privacy, data protection and safety online are protected under Nigeria's and South Africa's regulatory frameworks. The scholar evaluated and specifically compared Nigeria's and South Africa's frameworks and case law with the frameworks of the EU and United States and case law in order to deduce insights and lessons. Arowolo finds that although both Nigeria and South Africa have made significant progress in safeguarding the privacy and safety of children online, the regulatory frameworks remain below the standards required by international law and African regional norms. She advances suggestions to bridge the gaps in the existing laws.

Without a doubt, all contributions in this volume align with and advance the objectives of the *Journal* in significant ways. The editorial board extends its profound gratitude to the scholars and experts who graciously peer reviewed articles in this volume in order to ensure the quality of the *Journal*. We look forward to working with you again in the future.

Dr Akinola E. Akintayo
Editor-in-chief
April 2025

African Journal on Privacy & Data Protection

To cite: M Raji, D Wilder, V Ugwuoke & M Bashir 'An assessment of the enforcement mechanisms in African data protection laws' (2025) 2
African Journal on Privacy & Data Protection 1-40
https://doi.org/10.29053/ajpdp.v2i1.0002

An assessment of the enforcement mechanisms in African data protection laws

*Mubarak Raji**
PhD student, School of Information Sciences, University of Illinois at Urbana-Champaign, USA

*Devyn Wilder***
PhD student, School of Information Sciences, University of Illinois at Urbana-Champaign, USA

*Valentine Ugwuoke****
PhD student, School of Information Sciences at University of Illinois Urbana-Champaign, USA

*Masooda Bashir*****
Associate Professor, School of Information Sciences; Associate Professor, Coordinated Science Laboratory and Information Trust Institute; Adjunct Assistant Professor, Department of Industrial and Enterprise Systems Engineering, University of Illinois at Urbana-Champaign, USA

* LLB (Bayero) BL (Lagos) LLM (Illinois); mraji2@illinois.edu. We thank Professor Madelyn Rose Sanfilippo, Muhammad Hassan of the University of Illinois School of Information Sciences, and Professor Faye Jones of the University of Illinois College of Law for reading and providing helpful feedback on the draft. We also appreciate the anonymous peer reviewers for their valuable comments.
** BS (Virginia Commonwealth University) MLIS (University of Washington Information School); dwilder2@illinois.edu
*** LLB (Nigeria) BL (Lagos) LLM (Illinois); ugwuoke2@illinois.edu
**** PhD (Purdue University); mnb@illinois.edu

Abstract

Africa has the second-biggest population in the world, with about 1,1 billion projected internet users by 2029. This growth in internet users has made many Africans vulnerable to privacy threats. To protect their citizens' personal data, about 38 out of 55 African countries have legislated data protection laws. While previous literature has provided valuable insights into African DPLs, most studies have focused on summarising the legal framework or comparing them to other legislations like the General Data Protection Regulation. Therefore, there is a significant gap in understanding African DPL enforcement mechanisms. Our study seeks to address this gap by identifying common, unique trends and practices in African DPL enforcement. To conduct this research, we used a rigorous qualitative evaluation method of thematic content analysis involving three independent researchers. The researchers examined data protection laws of 20 African countries, which are publicly available in English, regarding their enforcement mechanisms. Our analysis indicates that all 20 countries require a dedicated data protection authority to enforce DPLs, and the laws apply to private and public sectors. To deter privacy violations, we observed that 85 per cent of the countries prescribe administrative sanctions; all the countries have provisions for financial and criminal sanctions; we also observed that 65 per cent of the countries studied allow data subjects to seek private right of action. Furthermore, all 20 countries in our sample require data controllers to register or notify data protection authorities before data processing; 55 per cent of the countries have extraterritorial reach provisions. We believe our research is a critical step towards evaluating African DPLs, which will guide policy makers, international organisations, compliance analysts, lawyers, legislators and technology companies involved in data collection and processing in African nations. By comparing the enforcement approaches among different African countries, our findings can shape future regional policy and data protection practices.

Key words: Africa; data protection; data protection authority; enforcement mechanism; sanctions

1 Introduction

Data is the foundation of the modern world that drives innovation and fuels the digital transformation, which underscores the importance of personal data in the twenty-first century. This emphasises the growing importance of personal data in the technological era, where it has become one of the most valuable resources. Data is crucial, and it is the foundation of modern technological advancements. This accurately reflects the reality that data has emerged as the driving force of innovation in our world, as information is power and integral to economic development and wealth creation.[1] Nowadays, personal data is easily accumulated

1 K Schwab *The fourth industrial revolution* (2016); S Zuboff *The age of surveillance capitalism : The fight for a human future at the new frontier of power* (2019); D Coleman 'Digital colonialism:

using the internet, and Africa is not left out of this global trend. Africa has the second-largest population in the world, with the number of internet users increasing rapidly to about 728 million estimated users in 2024 compared to previous years and potential room for growth projected to about 1,1 billion users in 2029.[2] African internet users account for the world's highest mobile data usage, with approximately 74 per cent of users accessing the internet through mobile devices for different activities such as social media, with Facebook as the most used platform, e-commerce, online banking and mobile payment.[3] The growth in internet penetration in Africa also encompasses the creation, use and sharing of ever more personal data.

With the rise in personal data generated across Africa, there is growing concern about how personal data is protected in the era of surveillance capitalism and digital colonialism. Surveillance capitalism has been defined as the 'new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales'.[4] It is the process by which technology companies accumulate vast amounts of data, often without obtaining informed consent of the data subject, in order to exert dominance, influence user behaviour, and target advertisements to make a profit.[5] Surveillance capitalism underscored how personal data are integral to innovation and a tool to control the market economy, which can lead to users' behavioural control and surveillance, making users of technology tools sacrifice their privacy in exchange for technology usage.

Surveillance capitalism involves many stages, starting from data collection to extraction. Personal data such as location data, frequently used applications and websites, online search queries, and other personal preferences or habits from technological devices, including mobile phones and smart devices (for example, smart home technologies and smartwatches) and social media platforms. The next stage is data analysis of these personal data using computer algorithms to determine individual preferences, profiling and envisage future behaviours. The personal data collected is treated as commodities, often commercialised and sold to advertising companies. Using predictive analytics, targeted and personalised ads, the advertisers recommend products to the consumer to influence and manipulate their decisions to make profits for technology companies. In the process, users' privacy is being eroded mostly due to the absence of consent and transparency.[6] One major example of surveillance capitalism is the Facebook-

---

The 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws' (2019) 24 *Michigan Journal of Race and Law* 417, 423.

2 'Statista 'Number of internet users in Africa from 2014 to 2029 (in millions) chart' 25 July 2023, https://www.statista.com/forecasts/1146636/internet-users-in-africa (accessed 8 July 2024).'

3 'Statista 'Internet usage in Africa', https://www.statista.com/study/115328/internet-usage-in-africa/ (accessed 8 July 2024).'

4 Zuboff (n 1) 7.

5 Zuboff (n 1); Coleman (n 1).

6 Zuboff (n 1); Coleman (n 1) 423-434.

Cambridge Analytica controversy, where Facebook users' the personal data were harvested without their consent. The personal data was profiled with personalised political ads targeted to manipulate and influence the political voting choice. The case later led to one of the most significant privacy violations globally, with many legal battles across different jurisdictions.[7]

On the other hand, digital colonialism is where enormous amounts of personal data are harvested for profit by big tech companies that exploit the lack of technology infrastructure, access to the internet, competition, and data protection laws. Coleman explained that digital colonialism is mainly targeted at underdeveloped and developing countries, mostly in the Global South, by powerful technology companies in the Global North. Some characteristics and factors that enable digital colonialism include the digital divide, data extraction and exploitation, and reliance on the Global North for digital infrastructure such as social media, cloud storage, internet services and undersea cables. Others include unequal economic powers and technological monopoly since much of the internet technologies are developed and controlled by the Global North.[8]

Digital colonialism has been described as another form of modern-day colonialism. Classic colonialism occurred with the exploitation of raw materials during the scramble for Africa and colonisation using imperial trading corporations such as 'the British South African Company, the Germany East African Company, the Imperial British East African Company, and the Royal Niger Company as conduit pipe' leading to a history of mistrust. For example, Facebook Free Basics and Google C-squared programmes have been described as examples of digital colonialism in Africa.[9]

While surveillance capitalism occurs globally, digital colonialism is mainly targeted at less-developed societies. However, both pose a risk to human privacy, aimed to acquire personal data and for profit. These may lead to the erosion of privacy in many ways as personal data is collected from digital devices, smart technologies, IoT systems and search engines, and social media to capture behavioural data, manipulate users' habits and choices and enhance technology surveillance through predictive algorithms.[10] Additionally, like other regions of the world, privacy threats expose Africans to vulnerability, such as cybercrimes, such as stolen identity and internet fraud and cyberattacks.

Furthermore, there has been an increase in reported data breaches by data controllers and processors and data protection authorities imposing sanctions on private organisations and government actors in Africa. The most recent incident

7 https://www.bbc.com/news/technology-64075067; https://www.ftc.gov/news-events/news/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving-consumers-about-collection-facebook (accessed 8 July 2024).
8 Coleman (n 1).
9 Coleman (n 1) 423-434.
10 J Silverman 'Privacy under surveillance capitalism' (2017) 84 *Social Research* 147.

is the investigation and imposition of Nigeria's US $220 million fine on Meta, arguably the most significant fine in Africa compared to other penalties, which average less than US $1 million.[11] Other prominent data protection violations in the last three years that have attracted imposition of sanctions include Sokoloan's case in Nigeria in 2021;[12] the Kenyan Office of Data Protection Commissioner's acceptable on Chinese Oppo mobile in 2022;[13] fines imposed on Africell mobile telecommunication company in Angola in 2023;[14] the Yango application case in Côte d'Ivoire in 2023;[15] Sincephetelo Motor Vehicle Accident Fund's fines on Eswatini in 2023;[16] and sanctions on the South African Department of Justice and Constitutional Development.[17] More recently; it was reported that there was the unauthorised sale of personal data domiciled with the National Identity Management Commission in Nigeria, which the government initially denied but has commenced investigations.[18] Also, there is a growing menace of data protection violations and harassment by online lending application companies with scenarios in Nigeria, Kenya and Ghana.[19] The above concerns make assessing the enforcement of data protection laws on the African continent crucial.

11 Reuters 'Nigeria fines Meta $220 million for violating consumer, data laws' 19 July 2024, https://www.reuters.com/technology/nigerias-consumer-watchdog-fines-meta-220-million-violating-local-consumer-data-2024-07-19/ (accessed 1 August 2024).

12 National Information Technology Development Agency 'NITDA sanctions SokoLoan for privacy invasion' 17 April 2021, https://nitda.gov.ng/nitda-sanctions-soko-loan-for-privacy-invasion/ (accessed 11 July 2024).

13 DataGuidance 'Kenya: ODPC fines Oppo KES 5M for non-compliance with enforcement orders' 23 December 2022, https://www.dataguidance.com/news/kenya-odpc%C2%A0fines-oppo%C2%A0kes-5m-%C2%A0non-compliance (accessed 11 July 2024); 'Oppo fined Sh5m for breaching data laws' *Business Daily Africa* 21 December 2022, https://www.businessdailyafrica.com/bd/economy/oppo-fined-sh5m-for-breaching-data-laws--4063118 (accessed 11 July 2024).

14 Angola Data Protection Authority 'APD fines AFRICELL 150 thousand US dollars for violating the personal data protection law', https://www.apd.ao/ao/noticias/apd-multa-africell-em-150-mil-dolares-norte-americanos-por-violacao-da-lei-de-proteccao-de-dados-pessoais-lpdp/ (accessed 11 July 2024).

15 DataGuidance 'Ivory Coast: ARTCI issues formal warning and orders deactivation of Yango app' 13 November 2023, https://www.dataguidance.com/news/ivory-coast-artci-issues-formal-warning-and-orders (accessed 11 July 2024); Telecommunications/ICT Regulatory Authority of Côte d'Ivoire 'Press release' 8 November 2023, https://www.artci.ci/index.php/33-actualites/informations/629-probables-enregistrements-des-communications-ou-echanges-a-l-interieur-de-vehicules-utilisateurs-de-l-application-denommee-yango-sans-information-prealable-ou-consentement-des-personnes-concernees.html (accessed 11 July 2024).

16 'SMVAF fined E150 000 for breaching Data Protection Act' *Eswatini Daily News*, https://swazidailynews.com/2023/09/15/smvaf-fined-e150-000-for-breaching-data-protection-act/ (accessed 11 July 2024); Eswatini Communications Commission 'SMVA SDPA final decision' 23 August 2023 https://www.edpa.org.sz/assets/documents/SMVA%20EDPA%20FINAL%20DECISION%20-%20AUGUST%202023.pdf (accessed 11 July 2024).

17 Information Regulator South Africa 'Media statement' 4 July 2023, https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf (accessed 11 July 2024).

18 Paradigm Initiative 'Major data breach: Sensitive government data of Nigerian citizens available online for just 100 Naira' 20 June 2024, https://paradigmhq.org/major-data-breach-sensitive-government-data-of-nigerian-citizens-available-online-for-just-100-naira/ (accessed 11 July 2024); 'FG commences NIN data leak probe' *Punch* 27 June 2024, https://punchng.com/fg-commences-nin-data-leak-probe/ (accessed 11 July 2024).

19 Ghanian Data Protection Commission 'Press statement', https://www.dataprotection.org.gh/media/attachments/2023/06/27/press-statement-by-the-dpc1.pdf (accessed 11 July 2024); Techcabal 'Kenya fines two digital lenders $20,000 for abusing user data', https://techcabal.

Also, technological advancement has significantly increased, and one approach to data protection around the globe is the enactment of data protection laws to protect data privacy, extending beyond the traditional scope of privacy. As Warren and Brandeis rightly predicted, mechanical devices could pose potential threats and enhance privacy invasion without adequate legal measures.[20] The prediction has led many countries, political and economic unions, corporate associations and international organisations to develop rules, regulations, conventions, treaties or laws to regulate data protection. Africa has emerged as one of the leading regions with various data protection laws enacted by countries, and while the world is not paying sufficient attention, the number of African countries with data protection legislations has dramatically increased.[21] Some African countries require their citizens' personal data to be protected even if the data is processed in a foreign country, which is similar to the European Union (EU) General Data Protection Regulation (GDPR), which mandates the safeguarding of EU citizens and residents' personal data outside the EU. This is another point of concern for data processors and controllers possessing the personal data of Africans around the globe to be cognisant of their respective approach to data protection regulation. Hence, compliance with these data protection laws needs to be examined.

As of 31 March 2024, 38 out of 55 African countries have taken drastic measures to protect personal data by enacting country-specific data protection legislations in addition to other international instruments concurrently in force across different African sub-regions. These international instruments are discussed in detail in part 2.3 below. It is remarkable and laudable that African countries have taken giant steps with the enactment of data protection laws. While legislating data protection laws (DPLs) is the essential step towards privacy protection, it is equally important to determine the enforcement mechanisms that ensure data controllers' and processors' adhere to the legalisations; otherwise, the purpose of enacting those laws will be futile. Much of the previous literature has examined the African international and regional approach to data protection regulation,[22]

com/2023/09/26/digital-lenders-fined-in-kenya/ (accessed 11 July 2024); 'Commission probes 400 cases of privacy breach in online loan apps' *Punch* 28 March 2024, https://punchng.com/commission-probes-400-cases-of-privacy-breach-in-online-loan-apps/ (accessed 11 July 2024).

20 SD Warren & LD Brandeis 'The right to privacy' (1890) 4 *Harvard Law Review* 193.

21 B Leyva & D Leippzig 'Africa's innovation – July developments signal attention must be paid to data privacy developments in Africa' 5 August 2022, https://www.mayerbrown.com/en/insights/publications/2022/08/africas-innovation-july-developments-signal-attention-must-be-paid-to-data-privacy-developments-in-africa (accessed 11 July 2024).

22 G Greenleaf & B Cottier 'International and regional commitments in African data privacy laws: A comparative analysis' (2022) 44 *Computer Law and Security Review* 105638, https://doi.org/10.1016/j.clsr.2021.105638; O Babalola 'Data protection legal regime and data governance in Africa: An overview' in B Ndemo and others (eds) *Data governance and policy in Africa* (2023) 83.

tracing the historical origin of data in Africa,[23] data protection authorities,[24] and the legal framework of regulating data protection in several African countries. However, this study intends to address the research gap in assessing the African enforcement patterns of national data protection laws, which is a critical gap in literature.

In this study, we examined the enforcement mechanisms of data protection laws in 20 African countries to assess how personal data are safeguarded and the possible repercussions of violating data protection legislative frameworks.[25] In addressing the method of enforcing the data protection laws, we asked the following research questions: What enforcement approaches do African countries use to ensure adherence to data protection laws? Who is saddled with the responsibility of enforcing these laws? What kind of sanctions are specified in the laws?

2 Background

2.1 Privacy and data protection

Privacy is a complex concept that lacks a universally-accepted definition, like several concepts in the social sciences.[26] Broadly speaking, privacy pertains to an individuals' capacity to manage who can access their personal data, including their body, family, home, communication or personal information.[27] Warren and Brandeis foresee the future when they argue that mechanical devices may cause potential threats and enhance privacy invasion if adequate legal measures capture the present-day reality of data privacy in the internet era.[28] Their work accounted for how the right to privacy was birthed from the rights to life, property, and 'to

23 AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law and Security Review* 78; AB Makulilo 'The context of data privacy in Africa' in AB Makulilo (ed) *African data privacy laws* (2016) 3; AB Makulilo (2016) (n 23) 192-204; KM Yilma 'The quest for information privacy in Africa: A review essay' (2017) 7 *Journal of Information Policy* 111; M Jimoh 'The quest for information privacy in Africa: A critique of the Makulilo-Yilma debate' (2023) 1 *African Journal of Privacy and Data Protection* 1.

24 O Babalola & G Sesan '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' (2021), https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-2.pdf (accessed 11 July 2024).

25 Benin, Botswana, Côte d'Ivoire, Egypt, Ghana, Kenya, Lesotho, Malawi, Mauritius, Nigeria, Rwanda, São Tomé and Príncipe, Seychelles, South Africa, Somalia, Eswatini, Tanzania, Uganda, Zambia and Zimbabwe.

26 DJ Solove 'A taxonomy of privacy' (2006) 154 *University of Pennsylvania Law Review* 477-564; O Babalola *Privacy and data protection law in Nigeria* (2021) 9; L Abdulrauf 'Do we need to bother about protecting our personal data? Reflections on neglecting data protection in Nigeria' (2014) 5 *Yonsei Law Journal* 166.

27 Several authors have given a broader conceptualisation and definition of privacy. See, generally, LA Bygrave 'Privacy and data protection in an international perspective' (2010) *Scandinavian Studies in Law* 165-200; DJ Solove 'Conceptualising privacy' (2002) 90 *California Law Review* 1087-1155; Abdulrauf (n 26).

28 Warren & Brandeis (n 20).

be let alone'[29] and how it was accepted under common law initially as a tortious liability.[30] The right to privacy was later codified as a fundamental human right to privacy under several international treaties, such as the Universal Declaration of Human Rights 1948 (Universal Declaration),[31] and national constitutions in Africa.[32]

Privacy can be classified into different types: 'bodily privacy'; 'spatial privacy or territorial privacy'; 'behavioural privacy'; 'proprietary privacy'; 'associational privacy'; 'intellectual privacy'; 'decisional privacy'; 'communicational privacy'; and 'informational privacy'.[33] Informational privacy is the focus of this study, which deals with collecting, processing, retaining and using personal data that can be used to identify an individual and how these personal data can be protected.[34] It is worth mentioning that the Universal Declaration broadly defined human rights to privacy and provided that '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.'[35] However, data protection focuses on a narrower perspective regarding privacy protection, which involves holistic and sociotechnical aspects of privacy protection, especially information privacy.[36]

Informational privacy is otherwise known as 'data privacy' or 'privacy' in North America, whereas it is referred to as 'data protection' in most European legislations and literature.[37] In most African literature and legislation, the data privacy is described as data protection. Hence, the data protection nomenclature will be adopted in this work.

29 As above.
30 WL Prosser 'Privacy' (1960) 48 *California Law Review* 383.
31 Art 12 Universal Declaration of Human Rights (Universal Declaration). Other international instruments are the International Covenant on Civil and Political Rights (ICCPR) art 17; the Convention on the Rights of the Child (CRC) art 16; the European Convention on Human Rights art 8; the Charter of Fundamental Rights of the European Union art 7; the African Charter on the Rights and Welfare of the Child (African Children's Charter) art 10; the American Convention on Human Rights art 11; the American Declaration of the Rights and Duties of Man art 5; and the Arab Charter on Human Rights art 21. It is important to note that the right to privacy was not listed as a human right under the African Charter on Human and Peoples' Rights (African Charter), which is the major human rights treaty in Africa.
32 See the Constitution of the Federal Republic of Nigeria, 1999 sec 37; the Constitution of the Republic of Uganda, 1995 art 27; the Constitution of the Republic of Ghana 1992 art 18(2); the Constitution for the Republic of South Africa, 1996 art 14; the Constitution of the Republic of Kenya, 2010 art 31.'
33 'BJ Koops 'A typology of privacy' (2017) 38 *University of Pennsylvania Journal of International Law* 483; Babalola (n 26) 19-31; Abdulrauf (n 26) 168.
34 Abdulrauf (n 26) 168.
35 Art 12 Universal Declaration.
36 Bygrave (n 27) 167.
37 Bygrave (n 27) 166; Abdulrauf (n 26) 169; AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2 *International Data Privacy Law* 163.

2.2 Notion of privacy in Africa

There has been an ongoing debate about whether the notion of privacy is indigenous to Africa. For example, one champion of this debate is Makulilo.[38] He argues that the Western conception of privacy and individualism was imported to Africa, which influenced the development of privacy on the continent.[39] He buttresses his arguments with the fact that privacy rights were clearly omitted in the African Charter on Human and Peoples' Rights (African Charter), which indicated that privacy was not a popular concept.[40] He also argued that Africa has collectivist values relying on the concept of ubuntu, which originated from Southern Africa.[41] Ubuntu has been defined to mean that a person 'is part of a larger and more significant relational, communal, societal, environmental and spiritual world'.[42] Ubuntu encourages openness, community relationships, solidarity and transparency, while privacy can be termed 'secrecy', which is not in tandem with communalism values.[43] Several African societies have the equivalent of ubuntu and its communalism values, especially within families.[44] One way of conceptualising privacy in the Western world is that privacy is seen from an individual, personal space, autonomous, and personhood perspective, which is contrary to the concept of ubuntu, which underscores communal mindset, collective well-being, and communal accountability. The concept of ubuntu also raises the issues of collective privacy over personal privacy, where the conduct of a person can reveal the unique behaviour and identities of people in the families or communities.[45] For example, one of the ways to illustrate the communal approach to privacy is through the lens of genetic privacy. Imagine a family member shares their DNA for ancestral genetics; the individual's conduct can reveal the genetics of the entire family and make their genetics data available on the genetics database, which can be used to trace the ancestral origin, paternity and criminal investigation. It is essential to observe that the concept of ubuntu and the Western notion of privacy raise cultural perspectives and cross-continental approaches to privacy conceptualisation, which warrants further research through future studies.

38 AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law and Security Review* 78; AB Makulilo 'The context of data privacy in Africa' in AB Makulilo (ed) *African data privacy laws* (2016) 3.
39 Makulilo (n 37) 78; Makulilo (2016) (n 23) 192-204; Greenleaf & Cottier (n 22).
40 Makulilo (n 37) 78; Makulilo (n 38) 198.
41 Makulilo (n 37) 78; Makulilo (n 38) 194; Greenleaf & Cottier (n 22) 3-4.
42 JR Mugumbate & A Chereni 'Now, the theory of ubuntu has its space in social work' (2020) 10 *African Journal of Social Work* v.
43 HN Olinger and others 'We Western privacy and/or ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa' (2007) 39 *International Information and Library Review* 31.
44 Jimoh (n 23) 1.
45 U Reviglio & R Alunge 'I am datafied because we are datafied: An ubuntu perspective on (relational) privacy' (2020) 33 *Philosophy and Technology* 33, 595.

On the contrary, Yilma and Jimoh have countered Makulilo's argument that the theory of privacy was foreign to Africa.[46] They both argued that African societies are familiar with privacy, which is deeply rooted in their culture. Jimoh made some exciting illustrations to prove that privacy exists in several heterogeneous African societies and explained that in many family compounds, extended family members have their houses close to one another and have a common area. However, the homes are constructed in a way that respects the privacy of each nuclear or polygamous family in Yorubaland, predominantly in the southwest region of Nigeria and some parts of the Benin Republic.[47] He further buttresses his argument by using Àroko in the same Yoruba society, which is used in secret communication, indicating that privacy existed in pre-colonial Africa. Àroko utilised pre-packaged materials with symbolic elements to convey messages to those who understood the symbols.[48] He also cited the privacy values of the Amhara societies in present-day Ethiopia, where it is prohibited to enter another person's house without proper acknowledgement or being escorted inside, among other examples.[49] Yilma and Jimoh also contended that the mere fact the human right to privacy was omitted in the African Charter does not mean that privacy is alien to Africa, as posited by Makulilo, and can be described as an omission during the drafting stage.[50] Additionally, the fundamental right to privacy is already acknowledged in the constitutions of several African nations well ahead of the promulgation of the African Charter in 1981.[51]

Furthermore, most African countries were colonised by European countries. This shaped the legal systems of many African countries after gaining independence, mainly civil law or common law systems, legislative enactments, and the administration of justice.[52] After colonisation, the legislative frameworks in Europe still affect Africa. One clear example is the adequate level requirements under articles 25 and 26 of the EU Data Protection Directive 95/46/EC, which prohibited the transfer of Europeans' personal data to non-EU or foreign countries that did not fulfil the adequacy test, has an impact on data protection laws in Africa.[53] Also, some African countries are signatories and have ratified the Convention for the Protection of Individuals about Automatic Processing

46 Yilma (n 23) 111-119; Jimoh (n 23) 1.
47 Jimoh (n 23) 8.
48 As above.
49 Jimoh (n 23) 10.
50 Jimoh (n 23) 9; Yilma (n 46) 115.
51 Jimoh (n 23) 9; see Constitution of Nigeria, 1960 sec 23; Constitution of the Federal Republic of Nigeria, 1963 sec 23; Constitution of the Federal Republic of Nigeria, 1979 sec 34.
52 J Bryant 'Africa in the information age: Challenges, opportunities, and strategies for data protection and digital rights' (2021) 24 *Stanford Technology Law Review* 389-439 quoting SF Joireman 'Inherited legal systems and effective rule of law: Africa and the colonial legacy' (2001) 39 *Journal of Modern African Studies* 571.
53 Makulilo (n 37) 81, A Kusamotu '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' (2007) 16 *Information and Communications Technology Law* 149-159; AB Makulilo 'Data protection regimes in Africa: Too far from the European "adequacy" standard?' (2013) 3 *International Data Privacy Law* 42-50.

of Personal Data of the Council of Europe.[54] Additionally, Cape Verdean data protection law, which was the first national data protection law in Africa, was fashioned out of its colonial master, Portuguese data protection law, and France provided support to the Francophone African countries in developing their data protection laws.[55] Lately, many African countries have adopted the EU General Data Protection Regulation 2018 (GDPR) approach to data protection legislation. This can justify Bradford's postulation that Europe influences regulations in the world on data protection, anti-trust, and environmental sustainability, among others, which has been termed the 'Brussels effect'.[56] The above demonstrates that although external influences may hasten the development of data protection laws in Africa, privacy is not entirely new to some African societies.

2.3 African Union and regional data protection instruments

In the quest to safeguard and regulate personal data, there are three major approaches to data protection regulation in Africa, which can be categorised into the African Union (AU) approach, regional economic communities approach and national approach. In this part, we discuss several initiatives for data protection that are in place in Africa.

The African Union or continental approach is championed by the AU, a union of all 55 African countries.[57] The AU emerged from the Organisation of African Unity (OAU) that was initially created in 1963 to foster harmony and ensure collaboration among African countries.[58] In 2014 the AU adopted the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) on 27 June 2014 at Malabo, Equatorial Guinea.[59] The Malabo Convention contains provisions governing 'electronic transactions,'[60] 'personal data protection,'[61] and 'cybersecurity and cybercrime.'[62] Nineteen countries

54 The countries are Burkina Faso, Cape Verde, Mauritius, Morocco, Senegal and Tunisia. See Council of Europe 'Parties', https://www.coe.int/en/web/data-protection/convention108/parties (accessed 26 June 2024); L Abdulrauf 'African approach(es) to data protection law' in R Atuguba and others (eds) *African data protection laws* (2024) 31.

55 Bryant (n 52) 395.

56 A Bradford *The Brussels effect: How the European Union rules the world* (2020) 7.

57 Algeria, Angola, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cape Verde, Central African Republic, Chad, Comoros, Côte d'Ivoire, Democratic Republic of the Congo, Djibouti, Egypt, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Libya, Madagascar, Malawi, Mali, Mauritania, Mauritius, Morocco, Mozambique, Namibia, Niger, Nigeria, Republic of Congo, Rwanda, Sahrawi Arab Democratic Republic/Western Sahara, São Tomé and Príncipe, Senegal, Seychelles, Sierra Leone, Somalia, South Africa, South Sudan, Sudan, Tanzania, Togo, Tunisia, Uganda, Zambia and Zimbabwe. See African Union 'Member states', https://au.int/en/member_states/countryprofiles2 (accessed 27 June 2024).

58 African Union 'About the African Union', https://au.int/en/overview (accessed 27 June 2024).

59 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 27 June 2024).

60 AU Convention on Cyber Security and Personal Data Protection of 2014 (Malabo Convention) ch I.'

61 Ch II Malabo Convention.

62 Ch III Malabo Convention.

have already endorsed the Malabo Convention by signing it, and it entered into operation on 8 June 2023, approximately nine years following its adoption, when the fifteenth country ratified and deposited the Convention.[63] However, enforcing the Malabo Convention is a work in progress due to late ratification by at least 15 countries,[64] which made it in force nine years after its adoption and non-ratification by other countries, funding problems and absence of political will to ensure implementation.[65] Also, Africa does not have a continental or regional enforcement authority such as the European Data Protection Broad which may affect its effective implementation, mainly due to the nature of the Malabo Convention, which must be ratified first before becoming binding on any country, unlike the EU GDPR, which is binding and applicable in any EU country since it comes into force. Recently, the AU approved the AU Data Policy Framework in 2022.[66]

More recently, members of the Organisation of the African, Caribbean and Pacific States signed a Partnership Agreement with the EU and its member countries (Samoa Agreement) to advance human rights, the rule of law and democracy, enhance peace and security, and foster economic change, among others, on 15 November 2023.[67] Article 15 of the Samoa Agreement mandates parties to have adequate data protection legislation, monitoring enforcement, and establishing independent supervisory authorities.[68]

2.3.1 Regional economic communities' approaches

Africa is divided into five regional divisions: Central Africa, East Africa, North Africa, Southern Africa and West Africa. Some of these sub-regions formed regional economic communities to promote trade and economic harmony. These

63 Angola, Cape Verde, Côte d'Ivoire, Congo, Ghana, Guinea, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, and Zambia had ratified and deposited the Malabo Convention. Benin, Cameroon, Chad, Comoros, Djibouti, The Gambia, Guinea-Bissau, South Africa, Sierra Leone, São Tomé and Príncipe, Sudan and Tunisia are signatories to the Convention but have not ratified it. See African Union 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection' 19 September 2023, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf (accessed 27 June 2024).

64 The Malabo Convention stipulates that at least 15 countries must ratify it and deposit the ratification instrument to the AU for it to come into force. See Malabo Convention (n 60) art 36.

65 Greenleaf & Cottier (n 17) 10.

66 K Yilma 'African Union's data policy framework and data protection in Africa' (2022) 5 *Journal of Data Protection and Privacy* 1-7.

67 Council of the European Union 'Samoa Agreement: EU and its member states sign new partnership agreement with the members of the Organisation of the African, Caribbean and Pacific states' 15 November 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/11/15/samoa-agreement-eu-and-its-member-states-sign-new-partnership-agreement-with-the-members-of-the-organisation-of-the-african-caribbean-and-pacific-states/ (accessed 12 July 2024).

68 Council of the European Union 'Samoa Agreement', https://data.consilium.europa.eu/doc/document/ST-8372-2023-REV-1/en/pdf (accessed 12 July 2024).

regional economic communities have prescribed rules to guide data protection, and in this part we discuss some of the data protection initiatives.

Several African regional economic communities prescribed treaties or non-binding model laws for adoption by the participating countries. Prominent among them is the Economic Community of West African States (ECOWAS), which was established in 1975 and comprises 15 West African countries intending to foster 'economic integration' among participating states.[69] In 2010 the member states adopted the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS to govern data protection.[70] The law was the first regional data protection instrument to be in operation in Africa.[71]

The Southern African Development Community (SADC) is a Southern Africa-based regional economic community with 16 member states.[72] It was initially established as the Southern African Development Coordination Conference in 1980 to promote economic integration among member states.[73] The SADC prescribed the SADC Model Law on Data Protection in 2013,[74] produced as part of the International Telecommunication Union's Harmonisation of the ICT Policies in Sub-Saharan Africa project.[75] It is a model law for participating states to adopt and it is non-binding.[76]

The East African Community (EAC) is another regional bloc for political and economic cooperation with eight member states.[77] The EAC presented a draft of the EAC Legal Framework for Cyberlaws in 2008.[78] The frameworks contain provisions on electronic transactions, compute crime, consumer protection and data protection. The SADC Model Law is a guide for member states and is not a

69 ECOWAS 'About ECOWAS,' https://www.ecowas.int/about-ecowas/ (accessed 27 June 2024). The member states are Benin, Burkina Faso, Cabo Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Sierra Leone, Sénégal and Togo. See ECOWAS 'Member states', https://www.ecowas.int/member-states/ (accessed 27 June 2024).

70 https://www.statewatch.org/media/documents/news/2013/mar/ecowas-dp-act.pdf (accessed 27 June 2024).

71 Greenleaf & Cottier (n 22) 14.

72 Angola, Botswana, Comoros, Democratic Republic of the Congo, Eswatini, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, United Republic of Tanzania, Zambia and Zimbabwe are member states. See Southern African Development Community 'Member states', https://www.sadc.int/member-states (accessed 27 June 2024).

73 https://www.sadc.int/pages/history-and-treaty (accessed 27 June 2024).

74 Southern African Development Community 'History and treaty', 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 27 June 2024).

75 Greenleaf & Cottier (n 22) 15.

76 Babalola (n 22) 83.

77 See East Africa Community 'Overview of EAC', https://www.eac.int/overview-of-eac (accessed 27 June 2024). Member states are Burundi, the Democratic Republic of the Congo, Kenya, Rwanda, Somalia, South Sudan, Uganda, and Tanzania.

78 http://repository.eac.int/bitstream/handle/11671/1815/EAC%20Framework%20for%20Cyberlaws.pdf?sequence=1&isAllowed=y (accessed 27 June 2024).

binding authority.[79] With all these regional efforts, having a continental approach to enforcing data protection laws is still a work in progress due to non-ratification of the Malabo Convention 2014 and the need for a regional enforcement authority.[80]

2.4 National data protection laws

As stated earlier, some countries worldwide protect fundamental right to privacy in their national constitutions. About half of the 55 African countries enumerated privacy rights as one of the fundamental human rights protected in their constitutions.[81] The right to privacy broadly guarantees privacy in 'homes, correspondence, telephone conversations, and telegraphic communications,' but excludes clear provisions on data protection principles.[82] However, numerous African countries have passed data protection laws to ensure data controllers and processors lawfully acquire, control, store and process their citizens' personal data. For example, Cape Verde became the first African nation to enact data protection laws in 2001, and several other countries followed suit. As of the end of March 2024, 38 African countries have enacted data protection legislations, while 17 countries have not passed data protection laws. See Figure 1 for African countries with and without data protection laws and Figure 2 for the year of enactment of each data protection law in Africa. However, Cameroon, Djibouti, Ethiopia and Namibia have drafted data protection bills pending passage into law.[83]

79 Greenleaf & Cottier (n 22) 16.
80 Abdulrauf (n 54) 38; Greenleaf & Cottier (n 22); Yilma (n 66).
81 Greenleaf & Cottier (n 22) 6. The countries are Burkina Faso, Burundi, Chad, the Democratic Republic of the Congo, Egypt, Eritrea, Ethiopia, Guinea, Guinea-Bissau, Kenya, Lesotho, Liberia, Libya, Malawi, Mali, Mauritania, Morocco, Namibia, Nigeria, Rwanda, São Tomé and Príncipe, Sierra Leone, South Africa, South Sudan, Sudan, Tanzania, Uganda and Zimbabwe.
82 Sec 37 Constitution of the Federal Republic of Nigeria, 1999.
83 D Tsebee & R Oloyede 'Roundup on data protection in Africa – 2023', https://www.techhiveadvisory.africa/report/roundup-on-data-protection-in-africa---2023 (accessed 27 May 2024).

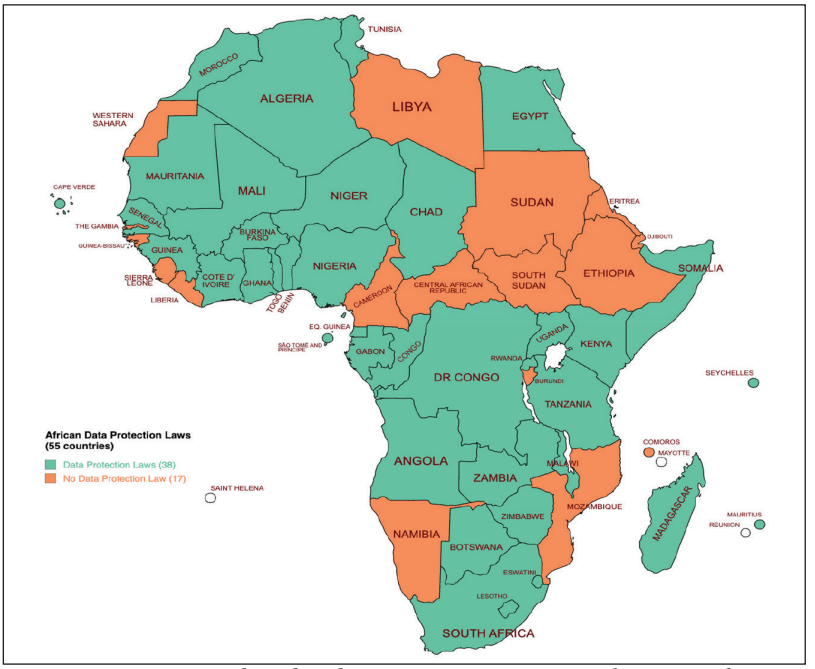

Figure 1: Countries with and without Data Protection Legislation in Africa

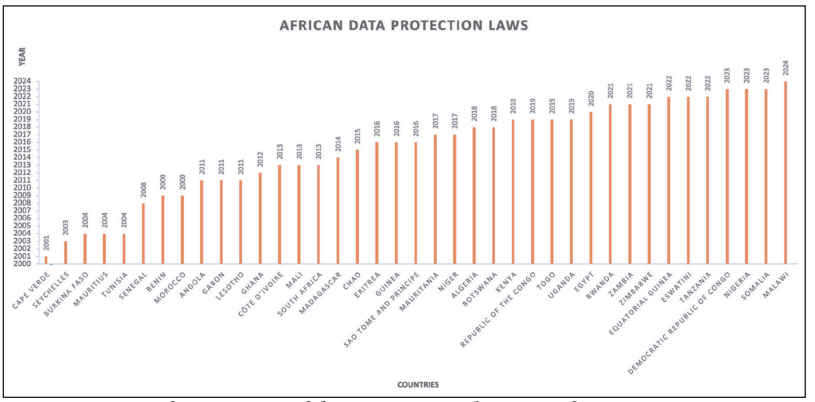

Figure 2: Year of enactment of data protection laws in Africa

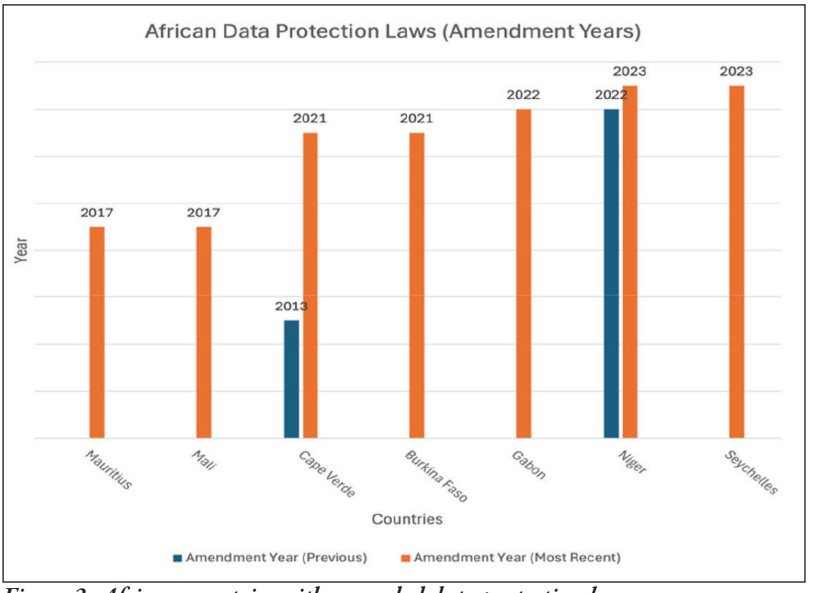

Figure 3: African countries with amended data protection laws

It is also imperative to observe that about seven countries have amended their data protection legislations after its first enactment. The countries are Cape Verde,[84] Seychelles,[85] Burkina Faso,[86] Mauritius,[87] Gabon,[88] Mali[89] and Niger.[90] For details, see Figure 3 above for the years of the amendment.

2.5 Enforcement of data protection laws

In an ideal society, all and sundry are expected to obey laws; however, legislators envisage that there will be violators. Hence, data protection laws prescribe some enforcement methods to ensure compliance and consequences of violations and non-compliance in the form of sanctions. Enforcing data protection laws involves some key players, measures and consequences of non-compliance. Under the comprehensive data protection approach, an enforcing body is saddled with the responsibility of monitoring, administering, regulating, enforcing and

84 DataGuidance 'Cape Verde', https://www.dataguidance.com/jurisdiction/cape-verde (accessed 12 July 2024).
85 Seychelles Data Protection Act 24 of 2023.
86 DataGuidance 'Burkina Faso', https://www.dataguidance.com/jurisdiction/burkina-faso (accessed 12 July 2024).
87 Mauritius Data Protection Act 20 of 2017.
88 DataGuidance 'Gabon', https://www.dataguidance.com/jurisdiction/gabon (accessed 12 July 2024).
89 https://apdp.ml/en/loi-ndeg2017-070-du-18-dec-2017-portant-modificatiion-de-la-loi-ndeg-2013-015-du-21-mai-2013 (accessed 12 July 2024).
90 DataGuidance 'Niger – Data protection overview', https://www.dataguidance.com/notes/niger-data-protection-overview (accessed 12 July 2024).

implementing data protection laws and overseeing personal data collection, storage, transfer, and lawful processing against the private and government sectors.[91] This enforcing body is mainly called data protection authority (DPA) or independent supervisory authority. This is comparable to article 51 of the EU GDPR, which mandates that EU member countries have a supervisory authority. However, the South African Protection of Personal Information Act (POPIA) mandates the establishment of the Information Regulator. Data protection authorities can issue regulatory guidance or regulation under data protection laws, oversee data protection compliance, investigate personal data violations and impose sanctions. Data protection authorities can also register data controllers and processors and maintain the register of controllers and processors. However, it is essential to observe that this registration is only mandatory if the country requires it.[92] In this study, we assess whether 20 African data protection laws have provisions for establishing independent data protection authorities or designating an existing government agency as DPA. We also looked at whether the DPA can register data controllers and processors. Some African countries, notably Nigeria and South Africa, have already established independent DPAs. In contrast, countries such as Eswatini, Zimbabwe and Rwanda have designated existing government entities and agencies as supervisory authorities.[93]

Sanction is the 'provision that gives force to a legal imperative by either rewarding obedience or punishing disobedience'.[94] In other words, sanctions are an enforcement mechanism with the force of law. It penalises non-compliance to deter an unlawful act and encourages obedience to law and order. Sanctions can be administrative, civil, financial or criminal sanctions.[95]

A sanction is administrative when ordered and imposed by a data protection authority, an administrative body, and not by a court of law, which can be informed of administrative penalties.[96] The court imposes civil sanctions as compensation or remedy to the plaintiff (data subject) for the injury caused by the defendant (violators of data protection laws), which is a form of a civil remedy or privacy right of action.[97] A data subject for which a data controller or processor has violated their data protection rights can institute a civil action against the violator before a court and will be entitled to damages as compensation without prejudice to other administrative remedies available with the supervisory authority is a classic example of civil sanction.[98]

91 P Swire & D Kennedy-Mayo *US private-sector privacy: Law and practice for information privacy professionals* (2020) 19.
92 Sec 44 Nigerian Data Protection Act 37 of 2023; sec 57 Protection of Personal Information Act 4 of 2013.
93 Abdulrauf '(n 58) 37-38.
94 WG Voss & H Bouthinon-Dumas 'EU general data protection regulation sanctions in theory and in practice (2021) 37 *Santa Clara High Technology Law Journal* 15, quoting B Garner *Black's law dictionary* (2019).
95 Voss & Bouthinon-Dumas (n 94) 16-17.
96 Voss & Bouthinon-Dumas (n 94) 18.
97 Voss & Bouthinon-Dumas (n 94) 19.
98 Arts 79 & 82 General Data Protection Regulation.

Financial sanctions involve paying money as a penalty, mainly in the form of fines for violating data protection laws.[99] Under EU GDPR, the supervisory authority has the power to investigate data breaches and impose administrative fines of '20 000 000 EUR, or in the case of an undertaking, up to 4 per cent of the total worldwide annual turnover of the preceding financial year, whichever is higher' can be classified as a financial sanction.[100] It is imperative to mention that a financial sanction can be an administrative sanction if it is imposed by a data protection authority and a criminal sanction if the court imposes it. A criminal sanction data violator is charged, prosecuted, evidence tendered, convicted, and sentenced to prison or a fine imposed.[101] The enforcement approaches of data protection laws in 20 African countries will be evaluated based on administrative, civil, financial or criminal sanctions.

These laws specify who is responsible for enforcement and prescribe some enforcement mechanisms to ensure compliance and sanctions for violators. The African countries' enforcement approach will be assessed based on whether they are administrative or civil sanctions, which are acceptable in the EU, or criminal sanctions, which are another form of sanction. The research questions and hypotheses for this topic are provided in this article under the introduction.

3 Related work

In the last two decades, several authors have written on legal frameworks for African data protection. Similarly, several African countries have enacted new data protection laws in the evolving legal space. Notably, existing literature in Africa focuses on the historical account of data protection,[102] international and regional instruments on data protection,[103] data protection authorities,[104] cross-border transfer of data,[105] and the legal framework of regulating data protection in several African countries, with Makulilo championing the discourse.[106] While

99 Voss & Bouthinon-Dumas (n 94) 17.
100 Art 83(5) General Data Protection Regulation.
101 Voss & Bouthinon-Dumas (n 94) 19.
102 AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer Law and Security Review* 78-89; AB Makulilo 'The context of data privacy in Africa' in AB Makulilo (ed) *African data privacy laws* (2016) 3-23; AB Makulilo 'A person is a person through other persons—A critical analysis of privacy and culture in Africa' (2016) 7 *Beijing Law Review* 192-204; Yilma (n 23) 111; Jimoh (n 23) 1-17.
103 Greenleaf & Cottier (n 22); Babalola (n 22) 83; M Fidler 'African data protection laws: Politics, but as usual' in R Atuguba and others (eds) *African data protection laws: Regulation, policy, and practice* (2024) 55-73.
104 O Babalola & G Sesan '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' (2021), https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-2.pdf (accessed 11 July 2024).
105 J Wanjiku & T Khaoma 'A case for continental cooperation in the harmonisation of a regional legal framework for cross-border data transfers in Africa' (2023) 1 *African Journal of Privacy and Data Protection* 18- 49.
106 See generally AB Makulilo (ed) *African data privacy laws* (2016).

we could not find prior studies examining several enforcement mechanisms of African data protection laws, we will review relevant articles related to this topic.

More specifically, Babalola and Sesan examined the role of data protection authorities as independent supervisory authorities in 30 African countries in enforcing data protection laws from 2007, when Burkina Faso first established a data protection authority in Africa, to 2021.[107] They analysed countries that have created data protection authorities, the mode of appointing officials to determine their independence and interference from their government, investigations carried out, decisions taken and transparency in enforcing data protection laws. This report is relevant to our study as it underscores the importance of data protection authority in enforcing data protection laws.

In another study by Bryant, he discussed the drawbacks, prospects and state of data protection in Africa in the technology era.[108] He submitted that colonialism and external influence aided the development of data protection laws in Africa.[109] He briefly discussed the legal framework of data protection in Ghana, Nigeria, Tunisia, South Africa, Mauritius and Angola.[110] He identified non-enforcement and misuse of personal data in the public sector and enforcing data protection on multinational companies as a significant challenge.[111] He also argued that external actors, mainly the West and China, may expose Africa to more vulnerability.[112] He concluded by recommending, among other things, the need for effective enforcement to ensure compliance with data protection laws.[113] His work is one of the motivations for this study, and it is relevant to examine whether the government actors are bound by data protection laws and enforcement patterns in 20 African countries.

In a more recent article, Abdulrauf discussed African data protection legislation approaches.[114] He argued that external influence, especially the EU and internal influence, especially African regional instruments, affects the approach to data protection regulation, and some countries have created supervisory authorities to enforce data protection laws and identified that some countries mandate government department to administer data protection law instead of creating an independent data protection authorities.[115] He enumerated some approaches, such as protecting vulnerable groups, alternative dispute resolution, and legislation in the local African language.[116] He made a case for the

107 Babalola & Sesan (n 104).
108 Bryant (n 52) 389-439.
109 Bryant (n 52) 393-395.
110 Bryant (n 52) 398-410.
111 Bryant (n 52) 410-416.
112 Bryant (n 52) 424-430.
113 Bryant (n 52) 437.
114 Abdulrauf (n 54) 38-39.
115 Abdulrauf (n 54) 35- 37.
116 Abdulrauf (n 54) 40-43.

Africanisation of data protection laws.[117] His work is related as it focuses on more general approaches to data protection. Hence, this article pays more attention to enforcement approaches.

Voss and Bouthinon-Dumas explained the concept of sanctions under the EU GDPR.[118] They stated that supervisory authorities can enforce the GDPR and could impose sanctions. They further argued that the GDPR has extraterritorial applicability, which affects the United States tech companies; hence, there is a need for these companies to comply with the GDPR to avoid huge sanctions just like sanctions previously imposed under EU competition law.[119] They explained the kinds of sanctions, including administrative sanctions imposed by data protection authorities as government agencies, financial sanctions in the form of money for GDPR violations, regulatory sanctions that can be enforced on companies that are regulated by regulatory authorities, civil sanctions gives data subject private right to action to approach the court for remedies, criminal sanction is imposed after criminal prosecution and conviction.[120] They argued that sanctions could be for rehabilitation, retribution, reparation, confiscatory, expressive or normative functions, deterrence or incapacitation.[121] They also considered the sanctions under the EU data protection directive and GDPR.[122] It is important to note that their work examining enforcement approaches was a motivating factor for this study.

4 Methodology

This study was a qualitative study examining the various approaches to enforcing data protection laws enacted in 20 African countries from 2000 to 2024, which were publicly available online and available in the English language to be able to conduct thematic content analysis, followed by the development of a structured coding strategy. After conducting preliminary analyses, three co-authors independently reviewed and analysed the 20 selected data protection laws based on a codebook developed for this study as independent researchers.

In our research on identifying data protection laws in Africa, we identified 38 African countries out of 55 that have enacted data protection laws as of March 2024. Upon downloading all the laws, we observed that some laws were in English and other languages (Arabic, Portuguese, French and other African languages). Hence, it was determined that we would only examine the laws that had an English language version publicly available as an inclusion criterion for the law to be analysed in this study. Thus, we focused our analysis on the 20 African countries

117 Abdulrauf (n 54) 44-51.
118 Voss & Bouthinon-Dumas (n 94) 1-96.
119 Voss & Bouthinon-Dumas (n 94) 4-16.
120 Voss & Bouthinon-Dumas (n 94) 17-20.
121 Voss & Bouthinon-Dumas (n 94) 23-45.
122 Voss & Bouthinon-Dumas (n 94) 45-68.

with an English version of their law that can be downloaded online. We excluded any laws that did not have an English version as of March 2024 to effectively determine their enforcement patterns. The English criterion was introduced because the research was conducted at a Midwestern university in the United States, and all the researchers were fluent in English. This criterion enabled them to examine and analyse the laws critically and directly from the published version without translation bias or oversight. It also enabled the researchers to conduct consistent comparisons of these laws to observe and identify common, unique trends and practices in enforcing data protection laws in Africa using a common language among them. Therefore, we acknowledge that our findings represent only the 20 countries included in this study and hence it may not generalise to all the 55 African countries. Nonetheless, we did ensure that all the five sub-regions in Africa, Central Africa, East Africa, North Africa, Southern Africa and West Africa, are represented in this study to be inclusive of the various regions.

The 20 countries selected for this study include Benin, Botswana, Côte d'Ivoire, Egypt, Eswatini, Ghana, Kenya, Lesotho, Malawi, Mauritius, Nigeria, Rwanda, São Tomé and Príncipe, Somalia, Seychelles, South Africa, Tanzania, Uganda, Zambia and Zimbabwe.

The following parts describe the scientific and systematic approach we used to conduct this research.

Step 1– Gathering African data protection laws

To identify and determine which African countries have data protection laws, we commence the research by reviewing existing literature and reports on African data protection laws.[123] We also conducted an extensive internet search to identify websites and repositories that will include African data protection laws, such as the United Nations (UN) Trade and Development (UNCTAD),[124] Morrison Foerster,[125] DLA Piper,[126] Data Protection Africa,[127] OneTrust Data Guidance,[128] and International Association of Privacy Professionals (IAPP)[129] websites. In collating the data protection laws, we utilised the IAPP Resource Centre and OneTrust Data Guidance (regulatory research software) as of March 2024 to ensure we had the same set of laws. The two databases led us to the same

123 Abdulrauf (n 26); Abdulrauf (n 54); Babalola (n 26); Babalola & Sesan (n 104); Bryant (n 52); Jimoh (n 23); Makulilo (n 102); Yilma (n 23).
124 United Nations Trade and Development 'Data protection and privacy legislation worldwide', https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed 29 May 2024).
125 M Foerster 'Privacy library', https://www.mofo.com/privacy-library (accessed 29 May 2024).
126 DLA Piper 'Data protection laws of the world', https://www.dlapiperdataprotection.com/ (accessed 29 May 2024).
127 Data Protection Africa, https://dataprotection.africa/ (accessed 29 May 2024).
128 OneTrust DataGuidance 'Africa', https://www.dataguidance.com/jurisdiction/africa (accessed 29 May 2024).
129 International Association of Privacy Professionals 'Global privacy law and DPA directory', https://iapp.org/resources/global-privacy-directory/ (accessed 28 May 2024).

countries' official websites, where the laws were downloaded. However, there was an exception in the case of Egypt, where there was no link to the country's government website; the law was downloaded from the IAPP Resource Centre.

We took measures to ensure that we selected the official and most recent versions of the laws by comparing the different files available on the repositories and resources we accessed, ensuring that the version we analysed was the official version released by the government of the selected countries. It is important to note that data protection laws are an evolving landscape in Africa. Therefore, in this study, the version of the reviewed and analysed laws was publicly available as of March 2024. See Figure 1 above for the list of African countries with or without data protection laws.

Step 2 – Examining the enforcement section and development of the codebook

Upon selecting the 20 countries to be further evaluated in the study, we initially read through the laws for the common themes and trends in enforcing data protection laws, which served as the basis for developing our codebook. The codebook was created to ensure objective and effective analysis, comparison of specific criteria examined, and consistent evaluation of each selected data protection law. The table below provides the specific criterion examined. For a description of what each criterion entails, see step 3 below.

Country	Legislation	Enactment Date	Data protection authority	Administrative Sanction	Financial Sanction	Criminal Sanction	Civil Action Register of Data Controller
Register of Data Controller	Extraterritorial Applicability	Compliance Audit	Applicability (Government or Industry)				

We created a codebook listing each of the 20 countries. For each country, three independent researchers reviewed and analysed the enforcement sections for the following criteria and coded them as either 'Yes' or 'Not mentioned'. For those criteria coded as 'Yes', we also noted the specific language, variation in description, similarities, and differences for each country and across the countries included in our study.

Each researcher made their coding independently for each of the selected countries before sharing their analysis with other researchers. If there was a

disagreement in coding any criteria, a group meeting was scheduled with the PI to discuss the discrepancies and reach a consensus if needed.

After the three independent researchers concluded reviewing the laws and coding, they met and agreed to label their findings in a separate codebook for inter-rater reliability. In labelling, two code definitions were used; the word 'Yes' stands for when the laws expressly or implied mentioned an act and 'Not mentioned' stands for issues not covered in the statutes or unclear.

In order to assess the agreement between the three raters, we decided to use Fleiss' Kappa for overall distributions, a statistical method for calculating reliability. Upon finishing the assignment of labels in the first iteration, each rater returned spreadsheets where all data was moved into a singular spreadsheet. Using RStudio and library package 'irr' containing the Fleiss' Kappa function, the calculation initially resulted in 0,35 or 35 per cent agreement among the three raters. Interpreting the results, an agreement of 35 per cent meant 'fair agreement' between the three raters. Due to a lower percentage of agreement, we decided on a second iteration consisting of a review or a process called rater monitoring and calculating results again.

For the second iteration, the raters unanimously agreed to reconnect to discuss the results of the labels. During this discussion, each rater was responsible for justifying their label and providing proof. If a rater had a label of 'Yes', there was documentation from said rater citing where the justification of the label would be located. A good illustration is a case of examining administrative and financial sanctions for Benin and Côte d'Ivoire, which were not easily comprehensible because the laws were originally drafted in French. Still, the data protection authorities have English versions on their website, which were relied upon. This usually included a section or article number used to identify the area. If a rater had a label of 'Not mentioned', there was no documentation provided signifying its absence.

Additionally, we validated our application of a consistent definition for each category, and the primary discussion was about implied statements versus explicit statements. Upon further analysis, the research team decided to mark a criterion as 'Yes' only if there was explicit content supporting those criteria. Therefore, the three researchers conducted a second round of review and analysis of the laws to recode, and this second round yielded a higher level (77 per cent) of agreement among the raters. This higher level of agreement was achieved because instead each was asked to provide content justification or lack thereof for their codlings. In addition, there was a discussion among the raters about each criterion, and the ratter had the option of keeping or changing their label. A good example of this is examining administrative sanctions for Zimbabwe, where the raters are not unanimous even after a meeting. The Zimbabwe Data Protection Act law stipulates that the Zimbabwe Postal and Telecommunications Regulatory Authority POTRAZ must approach the court for any administrative act not in

compliance with data protection principles. Two of the raters do not consider this an administrative sanction.

It is important to note that there was no obligation for unanimous agreement or a rater to change their label. While we had a high agreement, we still wanted to investigate the 23 percent disagreement to better understand what may have led to those discrepancies. In the process of this discussion between the raters, after providing justification, each rater had the option of keeping or changing their label. There was no obligation for unanimous agreement or for a rater to change their label.

After completing the second iteration of labels, we ran Fleiss' Kappa in RStudio again, and the calculation resulted in 0,77 or 77 percent agreement among the three raters. This result indicated excellent agreement between the three raters. A 100 percent agreement could not be reached due to a lack of consensus during the discussions. One major contributing factor was the researchers examining a translated version of the laws and, therefore, facing the challenge of language and translation variations where the content was unclear, making it difficult to make a solid determination. We decided as a group to leave labels where they were if criteria could not be identified clearly.

Step 3 – Analysing the specific content of the enforcement section

We continued employing a rigorous qualitative evaluation method involving three independent researchers in this step, which focused on analysing the content of a given criterion once it was coded as the law addressing those criteria.

To determine whether a selected country has a data protection authority specified in their laws, we checked if the law mandates the creation of data protection authorities or designates an existing government agency as a regulator of the country's data protection sector. For example, section 1(1) of the Ghana Data Protection Act establishing a data protection authority for Ghana provides that 'there is established by this Act a Data Protection Commission'.

To determine if a sanction is administrative, we studied the laws to observe whether the data protection authority can prescribe any of these administrative sanctions: cessation; the temporary or final withdrawal of authorisation to process data; warning; notice to stop; order to carry out specified steps; refrain from an act; and administrative fines. For example, section 42(2) of the Malawian Data Protection Act stipulates:

> (2) The compliance order issued by the authority under subsection (1) may include any of the following –
>
> (a) an order requiring the data controller or data processor to comply with a specified provision of this act;

(b) a cease and desist order requiring the data controller or data processor to stop or refrain from doing an act which is in contravention of this act;
(c) an order requiring the data controller or data processor to pay compensation to a data subject affected by the action or inaction of the data controller or data processor;
(d) an order requiring the data controller or data processor to account for the profits made out of the contravention;
(e) an order requiring the data controller or data processor to pay an administrative penalty not exceeding k20,000,000; or
(f) any other order as the authority may consider just and appropriate.

Concerning financial sanctions, we looked for words such as a particular amount of money, financial sum, or percentage of the data controller's annual return of the preceding financial year. The financial sanction can be in the form of administrative or criminal fines.

Section 63 of the Kenyan Data Protection Act is apt on this, which provides:

> In relation to an infringement of a provision of this Act, the maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is up to five million shillings, or in the case of an undertaking, up to one per centum of its annual turnover of the preceding financial year, whichever is lower.

For civil sanctions, which allows the data subject, the victim of a data violation, to institute an action before a court against the data controller or processor to seek damages for the injury suffered, we checked the laws for words such as compensation, private right of action, civil remedies, and damages and their equivalents. A good instance of this is section 51 of the Nigerian Data Protection Act, which provides that '[a] data subject, who suffers injury, loss, or harm as a result of a violation of this Act by a data controller or data processor, may recover damages from such data controller or data processor in civil proceedings'.

As for criminal sanctions, we studied the laws to see if the laws prescribed offences and punishments, such as criminal fines, imprisonment terms, forfeiture, or words such as convict and crime, are contained in the law. Article 56 of the Rwandan Data Protection Act provides:

> A person who accesses, collects, uses, offers, shares, transfers or discloses personal data in a way that is contrary to this Law, commits an offence. Upon conviction, he or she is liable to an imprisonment of not less than one (1) year but not more than three (3) years and a fine of not less than seven million Rwandan francs (RWF 7 000 000) but not more than ten million Rwandan francs (RWF 10 000 000) or one of these penalties.

On registration of the data controller, we checked whether the mandated data controller registered with the data protection authorities before commencing processing personal data or whether the data protection authorities are mandated to keep the data controller's register. An illustration of this is captured under section 29 of the Ugandan Data Protection Act thus:

(1) The Authority shall keep and maintain a data protection register.
(2) The Authority shall register in the data protection register, every person, institution or public body collecting or processing personal data and the purpose for which the personal data is collected or processed.
(3) An application by a data controller or other person to register shall be made in the prescribed manner.

Also, we reviewed the laws to see whether they expressly specify applicability to public and private sectors or every controller without excluding the government. Specifically, section 3 of the Mauritius Data Protection Act provides:

(1) This Act shall bind the state.
(2) For the purposes of this Act, each Ministry or Government department shall be treated as separate from any other Ministry or Government department.
(3) This Act shall apply to the processing of personal data, wholly or partly, by automated means and to any processing otherwise than by automated means where the personal data form part of a filing system or are intended to form part of a filing system.
(4) This Act shall not apply to –
    (a) the exchange of information between Ministries, Government departments and public sector agencies where such exchange is required on a need-to-know basis;
    (b) the processing of personal data by an individual in the course of a purely personal or household activity.
(5) Subject to section 44, this Act shall apply to a controller or processor who –
    (a) is established in Mauritius and processes personal data in the context of that establishment; and
    (b) is not established in Mauritius but uses equipment in Mauritius for processing personal data, other than for the purpose of transit through Mauritius.
(6) Every controller or processor referred to in subsection (5)(b) shall nominate a representative established in Mauritius.
(7) For the purpose of subsection (5)(a), any person who –
    (a) is ordinarily resident in Mauritius; or
    (b) carries out data processing operations through an office, branch or agency in Mauritius, shall be treated as being established in Mauritius.

Lastly, to determine whether the laws have extraterritorial effects, we review the laws to see if they specify that the laws apply to data controllers or processors who are not domiciled in a country but process personal data of the country's residents. Section 2(1)(c) of the Nigerian Data Protection Act provides that 'the data controller or the data processor is not domiciled in, resident in, or operating in Nigeria, but is processing personal data of a data subject in Nigeria'.

5 Results

Data protection is an evolving landscape in Africa. As of March 2024, we could trace 38 out of 55 African countries having all-inclusive data protection laws and

17 countries without data protection laws.[130] Cape Verde was the first African nation to pass a data protection legislation, and Malawi was the latest country with the signing of the Malawian Data Protection Act in January 2024.[131] The list keeps increasing as some other countries have released data protection bills, which are waiting to be enacted into laws before their legislative houses.[132] Other results of our study will be presented in this part, and further explanations will be provided under discussions.

Among the 20 countries selected for this study, 15 had dedicated parts for enforcement with different legal terminologies, which are enumerated in the table below. However, we do not see dedicated parts for enforcement in five countries, such as Côte d'Ivoire, Mauritius, Seychelles, Zambia and Zimbabwe, but several sections of the laws contain enforcement provisions.

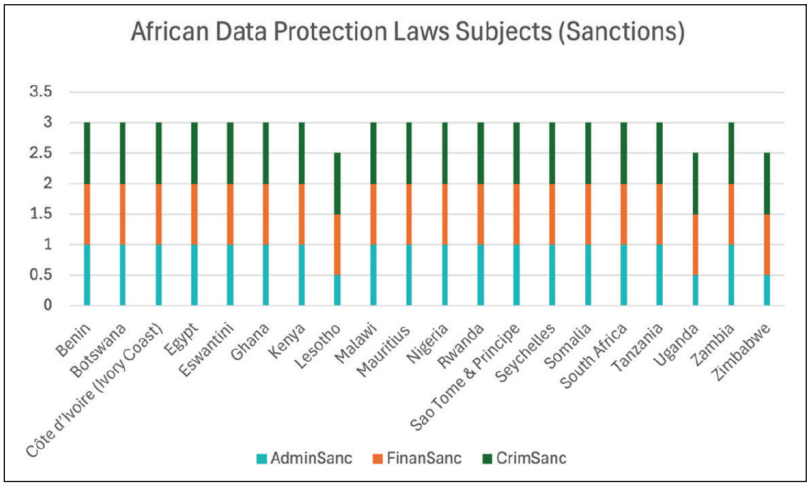

Figure 4: Administrative, financial and criminal sanctions by country

Figure 4 is a bar chart showing the classification of sanctions as administrative, financial and criminal sanctions by the 20 African countries we examined in this study. Regarding administrative sanctions, we observed that 17 of the 20 selected African countries empower the data protection authority to levy administrative sanctions for violating their data protection laws. However, there was some uncertainty for us in making a final determination on administrative sanctions for the three countries, Lesotho, Uganda, and Zimbabwe.

For financial sanctions, our analysis indicated that all 20 selected African countries authorise data protection authorities (in the form of administrative

130 See figure 1 above for African countries with data protection laws.
131 Malawi Data Protection Act 3 of 2024.
132 Eg, Ethiopia and Namibia have pending data protection bills.

sanctions) or the court (in the form of criminal sanctions) to impose financial sanctions on data controllers or processors who violate data protection laws.

Violations of data protection laws may attract criminal punishments. Our examination revealed that all the 20 countries selected in this study have provisions for criminal sanctions in their data protection laws.

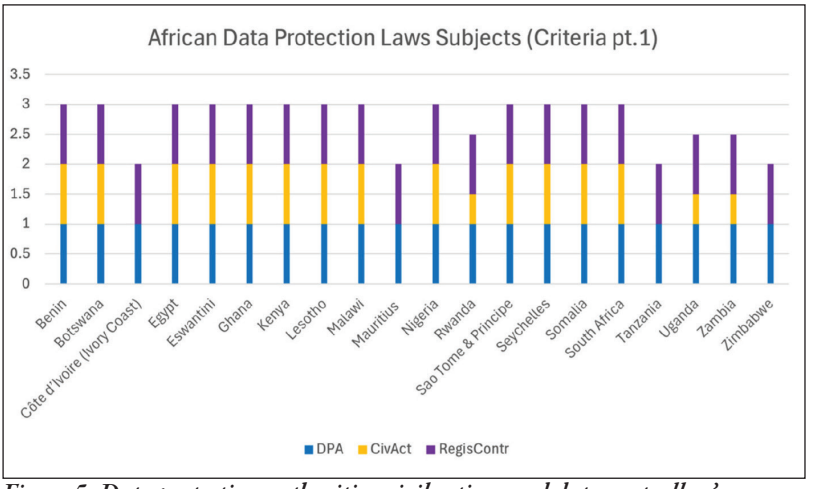

Figure 5: Data protection authorities, civil action, and data controllers' registration by country

Figure 5 is also a bar chart indicating countries that provide for the formation of data protection authorities to enforce data protection legislations, countries that allow data subjects to commence civil actions to seek compensation for damages resulting from data violations through civil remedies, and countries that mandate the registration of data controllers and processors or notification data protection authority before data processing the 20 African countries selected for this study.

Concerning the data protection authority, the three independent researchers agreed that all the 20 selected African countries in this study have provisions for establishing a data protection authority as the government agency saddled with responsibility for the administration, execution, and implementation of data protection laws in each country.

Concerning civil sanctions, our assessment revealed that a data subject has a private right of action in 13 out of 20 selected countries. The countries are Benin, Botswana, Egypt, Eswatini, Ghana, Kenya, Lesotho, Malawi, Nigeria, São Tomé and Príncipe, Seychelles, Somalia and South Africa. However, we cannot find civil sanctions in data protection laws in four countries: Côte d'Ivoire, Mauritius, Tanzania and Zimbabwe. However, there was uncertainty for us in making the

final determination for three countries' data protection laws containing civil sanctions or private rights of action: Rwanda, Uganda, and Zambia.

On registration of data controllers and processors, our review indicates that the selected 20 African countries mandate data controllers and processes to register or notify the data protection authority before controlling or immediately after collecting personal data.

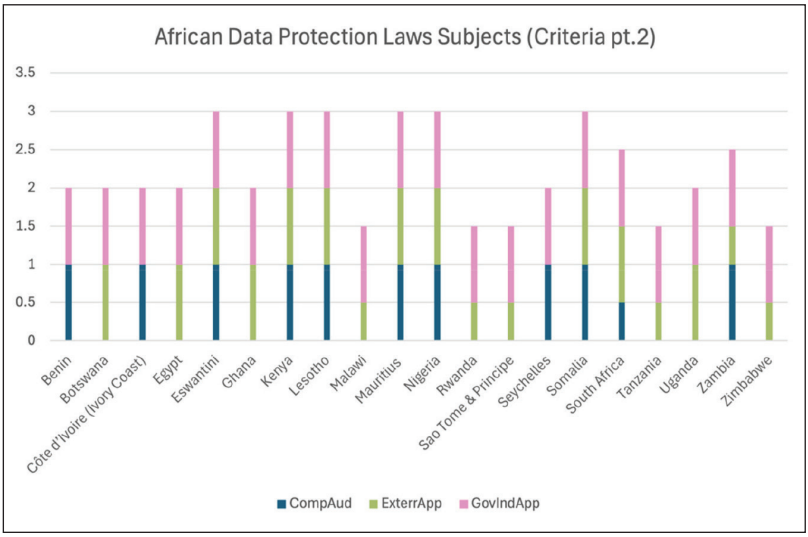

Figure 6: Compliance audit, extraterritorial applicability, and applicability by country

Figure 6 is another bar chart highlighting countries that make provision for regulatory compliance audits, countries whose laws have extraterritorial reach (meaning the laws are applicable beyond the countries' borders) and the applicability of data protection laws to the public and private sectors in the selected 20 African countries in this study. For a more detailed explanation, see the discussion in part 6 below.

Regarding compliance audit, we observed that nine out of the 20 countries, or 45 per cent of countries being assessed, did not have an explicit compliance audit process mentioned or outlined in their data protection laws, namely, Botswana, Egypt, Ghana, Malawi, Rwanda, São Tomé and Príncipe, Tanzania, Uganda and Zimbabwe. We observed that ten countries made provisions for compliance audits, including Benin, Côte d'Ivoire, Estwani, Kenya, Lesotho, Mauritius, Nigeria, Seychelles, Somalia and Zambia. However, there was uncertainty, and we could not make a final determination for South Africa.

We observed that data protection laws have extraterritorial effect provisions, meaning that data controllers or processors who are not domiciled in a country

but process personal data of the country's residents may be mandated to obey the country data protection law, just like the EU GDPR. Our review showcases that the data protection laws of 11 out of the 20 selected countries have extraterritorial effects. The countries are Botswana, Egypt, Eswatini, Ghana, Kenya, Lesotho, Mauritius, Nigeria, Somalia, South Africa and Uganda. Similarly, we could not find provisions on extraterritorial applicability in the data protection laws of 3 countries, namely, Benin, Côte d'Ivoire and Seychelles. However, there was uncertainty, which prevented us from making final determinations concerning six other countries, namely, Malawi, Rwanda, São Tomé and Príncipe, Tanzania, Zambia and Zimbabwe.

On the applicability of data protection laws to the public and private sectors, we observe in our study that the selected 20 data protection laws apply to both government and industry. In other words, data controllers and processors in the public and private sectors are obligated to adhere to data protection laws; otherwise, they will be liable if data protection laws are violated. However, the laws specify some exceptions in the applicability of data protection laws.

6 Discussion

6.1 Data protection authority

As stated above, we observed that the government plays a critical responsibility in data protection in Africa. The laws stipulated that data protection authorities, which are government agencies, should be established to monitor, administer, regulate, impose sanctions, prosecute violators, and enforce data protection laws. This is similar to what is obtainable under the EU GDPR, where the government-owned supervisory authority plays a crucial function in enforcing data protection laws. Out of the 20 countries selected in this study, 16 countries provide for establishing independent data protection authorities with different nomenclatures. The South African Information Regulator and the Kenyan Office of Data Protection Commissioner are good examples. However, four countries designated a department in existing ministries or agencies to enforce data protection laws, such as the Rwandan National Cyber Security Authority, Eswatini Communications Commission (ESCCOM), Zimbabwe Postal and Telecommunications Regulatory Authority and Malawi Communications Regulatory Authority.

The government, as the regulator of data protection in Africa, has some advantages, including ensuring regulatory compliance, enforcement, and implementation of data protection laws as part of its existing executive functions. This allows for effective coordination with other governmental agencies, such as the police and Information and Communication Commission, as well as competition and consumer protection agencies. Data protection authorities are

mostly independent and easily accessible to the public, enhancing public trust and accountability and preventing fraud and cybercrime.

However, it may also lead to excessive government control, such as censorship, limiting freedom of speech and other undemocratic government practices. The Nigerian government's banning of Twitter is a classic example.[133] Also, funding data protection authorities may not be the government's priority in some African countries due to infrastructure deficits and poor economic development, which may impact their ability to work effectively and hire qualified personnel to investigate data protection violations. Governmental administrative bottlenecks and lengthy procedures may hinder the effective execution of data protection laws. Additionally, the powers of the data protection authorities may be abused by introducing straining or overreaching regulations. The government appoints the boards of data protection authorities, which may give room for political influence in the agencies' administration. Meddling with the activities of the data protection authorities poses a major challenge to enforcing data protection laws significantly against foreign violators as it reduces confidence in the data protection authorities and may raise fear of victimisation, especially when the government is not a democratically-elected government.

6.2 Administrative sanctions

The data protection authorities can, on their own volition or upon the complaint of a data subject, investigate the violation of data protection laws and issue administrative sanctions. The nature of administrative sanctions includes notice of violation; cessation; the temporary or final withdrawal of authorisation to process data; warning; notice to stop; order to carry out specified steps or measures; refrain from an act; account for profit; compensation to victim; and administrative fines as a financial penalty specified by these African countries. However, the Zimbabwe Data Protection Act does not provide for administrative sanctions.[134] Still, it empowers the Zimbabwe Postal and Telecommunications Regulatory Authority to approach the court for any administrative act not in compliance with data protection principles, which takes away the power to levy administrative sanctions from the data protection authority.

The data controllers or processors are mostly notified of their violations and administrative sanctions through an enforcement or penalty notice prescribed by the data protection authority to remedy the breach within a stipulated period, which may also include a penalty. A violator dissatisfied with the administrative

133 CNN World 'Nigeria bans Twitter after company deletes President Buhari's tweet', https://www.cnn.com/2021/06/04/africa/nigeria-suspends-twitter-operations-intl/index.html (assessed 21 August 2024).
134 Sec 6(d) Zimbabwe Data Protection Act 5 of 2021.

sanctions may seek judicial review or appeal to the court within a specified period.[135]

Giving data controllers or processors notice of violation of data protection practices will make the violator address the complaint and avoid possible future violations by appropriate measures in changing their data protection practices. Also, the fear of sanctions, losing business reputation, public goodwill and customers can make data controllers improve their data proception practices and deter companies and governments from abusing personal data, which will prevent data violations and ensure compliance. However, delayed administrative processes may prolong the issuance of administrative sanctions. Likewise, investigation can be time consuming and requires technical expertise, which may not be readily available. For example, it took about two years for the South African Information Regulator to conclude the investigation and issue enforcement notice 2024 on TransUnion after security breaches were reported in March 2022.[136] Delays in the investigation of data protection laws may allow the violators to make profits before or during the investigation of the breach. The profit may not be accounted for if the country does not have an account for profit as an administrative sanction, such as Malawi, Nigeria and Somalia, which require data controllers to account for profit earned due to data protection violations.

6.3 Financial sanctions

As stated earlier, all 20 African countries have a form of financial sanction that is monetary. In these circumstances, violators of data protection laws pay money to the government for non-compliance with data protection laws. Financial sanctions may take the form of administrative fines of a particular amount or a prescribed percentage of the annual return of the data controller in the preceding financial year, as in the case of Kenya, South Africa, Rwanda and Nigeria. For example, the Kenyan Data Protection Act provides administrative fines for up to five million shillings or 1 per cent of annual turnover in the preceding financial year.[137] This is similar to what is obtainable under the EU GDPR, where data protection violators can be fined up to €20 000 000 or 4 per cent of the organisation's global annual revenue in the prior financial year. The significant difference is that the amount was specified in local currency, and the percentage, which we believe is within the peculiarity of each country. However, the administrative penalty in Somalia may be up to US $1 million or its equivalent amount.[138]

On the other hand, financial sanctions can be specified as fines levied upon conviction, a form of criminal sanctions in countries such as Lesotho,

135 Sec 64 Kenya Data Protection Act 24 of 2019; secs 97 & 98 South Africa Protection of Personal Information Act 4 of 2013; art 39 Somalia Data Protection Act 5 of 2023.
136 Information Regulator South Africa (n 11).
137 Sec 63 Kenya Data Protection Act 24 of 2019.
138 Art 37 Somalia Data Protection Act 5 of 2023.

Mauritius, Uganda, Zambia and Zimbabwe. Therefore, financial sanctions can be administrative sanctions if it is levied by the data protection authority and criminal sanctions if the court imposes them.

Financial sanction serves to generate revenue for the government. For this reason, several African countries will pay more attention to data protection practices in the coming years, especially with Nigeria's recent imposition of US $220 million on Meta for data protection and consumer practices violations. However, it may leave the victims without compensation for the data breach suffered in the absence of the data subject's private right of action and data protection law specifying the victim's compensation as an administrative sanction, as in the case of Malawi, Nigeria and Somalia.

While it is unclear how the violator may pay financial sanctions, it may perhaps be prescribed by the data protection authorities within their general powers of administration of data protection laws. Big corporations can easily afford to pay financial sanctions, like a pin of water in the ocean, especially if the fines were assessed in local African currency and the violators earned revenue in foreign currency. However, smaller corporations may be unable to afford the penalties. They may go bankrupt due to financial sanctions, which is imperative for companies, especially African fintech and start-ups, to take data protection practices seriously. Therefore, examining this aspect of the laws would be a good future study that would shed light on this issue.

6.4 Criminal sanctions

As stated earlier in the result above, all the selected 20 African countries have provisions for criminal sanctions, such as fines, forfeiture and imprisonment terms. Zimbabwe has additional sanctions such as seizure, data deletion and destruction of items.[139] Officers and directors of the data controller or processor may be individually criminally liable for violating data protection laws. For example, in Lesotho and Eswatini, if the data controller is a juristic person, the chief executive officer will serve the sentence of imprisonment term imposed on the data controller.[140] Corporate data controllers' employees involved in data protection violations will be personally liable and may be charged for a crime alongside the data controller.[141] Additionally, the partner may be jointly and severally liable in Zimbabwe and Zambia, extending this to unincorporated associations. In addition, data controllers can also be vicariously liable for violations caused by their employees, directors and officers.[142] Phrases such as 'juristic person' or 'legal person' and 'corporate body' were utilised in the laws, which may include public sector departments and agencies.

139 Sec 33 Zimbabwea Data Protection Act 5 of 2021.
140 Sec 55 Lesotho Data Protection Act of 2021; sec 53 Eswatini Data Protection Act of 2021.
141 Sec 50 Malawi Data Protection Act 3 of 2017; sec 76 Zambia Data Protection Act 3 of 2021.
142 Sec 51 Malawi Data Protection Act 3 of 2017.

Data protection authorities are mandated in most countries to prosecute crimes that contravene data protection laws. However, we observed that in Mauritius, the prosecution of offenders is subject to the permission of the director of public prosecution, which makes us wonder if this will not disturb the independence of the data protection authorities.[143]

Criminal sanctions will serve a deterrence function as they will make officers of the data controller exercise extreme caution and provide adequate measures while processing personal data, especially because of the personal liability effect. Just like financial sanction, it may not compensate the victim. Even though we did not encounter any criminal prosecution for violation of data protection laws in the selected 20 African countries, criminal sanction may be abused, especially for vendetta or abuse of office. An illustration is the ongoing prosecution of a Binance bitcoin American executive for money laundering after he had travelled to Nigeria to discuss regulatory compliance issues with the Nigerian government.[144] This is contrary to what is obtainable under the EU GDPR, which does not provide for the kind of criminal sanctions enumerated in the examined African data protection laws, as privacy violators cannot be charged with criminal offences in the EU. Additionally, the inefficiency of the administration of criminal justice poses challenges that can affect data controllers' both local and foreign confidence in the application of criminal sanctions as an enforcement mechanism of data protection laws.

6.5 Civil sanctions

Most countries empower data subjects to initiate legal action against data controllers or processors, seeking compensation before a competent court for damages as compensation for a resolution of violation of the data protection laws. The EU GDPR has an equivalence provision on the private right of action. However, there are some exceptions: Côte d'Ivoire, Mauritius, São Tomé and Príncipe, and Zimbabwe data protection laws does not specify the data subjects' rights to claim damages for privacy violations. Notably, Tanzanian law grants the Personal Data Protection Commission the authority to access compensation and order violators to make payments, which means the data subject will not go through the court system for compensation.

Civil sanction arguably is the best remedy for data subjects who suffered from data protection violations. The victim will be compensated for damage suffered from violating data protection laws. Damage may be extended to 'financial loss' and 'not involving financial loss' such as 'distress'.[145] It is imperative to note that

143 Sec 53(3) Mauritius Data Protection Act 2017.
144 'Binance executive denied bail in Nigeria over money laundering charges' *The Guardian*, https://www.theguardian.com/technology/article/2024/may/17/binance-executive-denied-bail-in-nigeria-over-money-laundering-charges (assessed 21 August 2024).
145 Sec 65(4) Kenyan Data Protection Act 24 of 2019.

we did not come across class action as a way of commencing private action against data protection violators in the 20 data protection laws examined. Even though we did not examine the civil procedure laws of each country, there is the likelihood that each data subject may have to instigate a lawsuit for data violation individually, which will increase the number of lawsuits pending before the courts, add to the judges' workload and may ultimately prolong the duration of administration of justice. However, whether data subjects can access justice using civil sanctions, private right of action, and lack of class action mechanisms can be the subject of another study as it requires empirical data, just like Muhawe and Bashir examined the effect of Article III standing on private right of action in the United States.[146]

6.6 Registration of data controllers and processors

In the selected African countries in this study, data controllers and processors are obliged to notify and register with the data protection authority before collecting, controlling and processing data or immediately after the collection. Failure to notify or register with the data protection authority is classified as violating data protection laws in many of the selected countries. However, Malawi, Nigeria and Somalia require data controllers or processors of 'major importance or significance' to register with the data protection authority, unlike the other countries that make registration mandatory for data controllers and processors.

Registration of data controllers will enable the data protection authorities to have a register of all data controllers and processors in each of the selected countries to monitor compliance. We observed that registration is required before personal data processing in countries such as Eswatini, Mauritius, South Africa, Tanzania, Zambia and Zimbabwe. However, in Nigeria and Somalia, data controllers or processors of major importance are obligated to register within six months of reaching the significant importance status.[147]

However, enforcing mandatory registration of data controllers will be challenging for African data protection authorities against data controllers and processors not resident in Africa but gather, store and process personal data emanating from Africa. For example, challenges such as identifying non-resident data controllers and, in the case of Nigeria, Malawi and Somalia, whether they are data controllers or processors of major significance.

146 C Muhawe & M Bashir 'Privacy as pretense: Empirically mapping the gap between legislative and judicial protections of privacy' (2023) *Illinois Journal of Law, Technology and Policy* 257.
147 Sec 44 Nigeria Data Protection Act 37 of 2023; art 32(1) Somali Data Protection Act 5 of 2023.

6.7 Compliance audit

Data protection authorities are empowered to conduct periodic data processing audits of data controllers and processors. The purpose of compliance audits under data protection laws is to ensure that data controllers and processors adhere to the laws. Notably, Nigeria, Somalia and Zambia allow data protection authorities to license third-party experts to carry out compliance services.

We observed that many countries, including those with an explicit compliance audit process, included language alluding to routine maintenance and risk assessment. We distinguished general maintenance from compliance auditing by acknowledging that audits signify periodic interventions, not routine impact assessments conducted by data controllers. Another trend noticed and documented in the acts was that traditionally, the audits were stated to be undertaken by either an outside organisation or assigned to a specific role where a phrase similar to 'is responsible for conducting periodic audits' is included.

Data controllers and processors are encouraged to employ internal data protection officers or contract organisations rendering data protection services to handle their internal audits before periodic audits by data protection authorities. This will ensure internal compliance and periodic staff training on data protection practices, which will prevent or reduce the effect of violating data protection laws. Additionally, countries such as Egypt, Eswatini, Ghana, Kenya, Malawi, Rwanda, Somalia, Uganda and Zimbabwe mentioned that data controllers might appoint data protection officers or supervisors.

6.8 Applicability of data protection laws

As stated earlier, we observed that all the 20 selected countries have ensured that their data protection legislations apply to the public and private sectors. This is mainly inferred from the applicability provisions. The Ghanaian Data Protection Act states that the law binds the state. However, there are some instances where data protection legislations are not applicable to every data processor or controller. The instances are personal or household purposes, national public health emergencies, legal claims and defence, criminal investigation and prosecution, public interest, national security and publication, among others.

One point of concern is how the data protection authorities ensure that governmental departments and agencies comply with data protection laws. We recommend that government employees be periodically trained on data protection practices and that each department have a dedicated data protection officer. It is illustrative to mention that the South African Information Regulator sanctioned the South African Department of Justice and Constitutional Development for

contravening the South African Protection of Personal Information Act.[148] This indeed is a laudable achievement, and we hope that other African countries can hold their public sector accountable as South Africa did. Specifically, we hope the Nigerian Data Protection Commission do the same with the allegation of personal data breaches by the National Identity Management Commission in Nigeria.

6.9 Extraterritorial applicability

As stated earlier under results, we observed that 55 per cent of the data protection laws we examined in this study have extraterritorial effects provisions. In other words, these countries stipulate that their data protection laws apply to non-resident data controllers or processors that process their citizens' personal data in the same way EU GDPR is binding on data controllers processing Europeans' personal data outside of Europe. As stated earlier, the extraterritorial stretch of data protection laws makes the data protection law in country A applicable and binding to data controllers or processors who are not residents of country A but collect, store and process the personal data of country A citizens. For example, the Nigeria Data Protection Act applies to 'the data controller or the data processor who is not domiciled in, resident in, or operating in Nigeria but is processing the personal data of a data subject in Nigeria.'[149]

These extraterritorial provisions in African data protection laws make it crucial for data controllers and processors, including big technology companies, educational institutions and banking and capital market actors that process Africans' personal data, to take drastic steps to familiarise themselves with these laws and ensure compliance. Additionally, Nigeria fined Meta US $220 million for non-compliance to data protection and competition laws in July 2024, which will serve as an eye opener to many African countries, and we envisage more African countries taking concrete steps to enforce their citizens' data protection rights as it serves as revenue generation.

7 Limitations and future study

As stated earlier, we utilised qualitative methods in carrying out this study, and like any other qualitative study, some limitations were introduced. To effectively analyse African data protection laws, we limited ourselves to each country's comprehensive data protection legislation enacted by the country's legislative body. Hence, we did not consider countries with the fundamental right to

148 Information Regulator South Africa 'Media statement', https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf (accessed 11 July 2024).

149 Sec 2(2)(c) Nigerian Data Protection Act 37 of 2023.

privacy in their constitutions but do not have a separate data protection law. Also, subsidiary legislation, such as regulations, directives and guidance issued by administrative agencies of the executive arm of government, was excluded. For example, both Uganda and Kenya released Data Protection Regulations in 2021 subsidiary legislation and were not considered in this study.

Additionally, the English language was a primary criterion for selecting the 20 countries in this study to determine their provisions properly. Hence, data protection laws without English versions publicly available were excluded from this study. We also limit ourselves to the latest version of the laws. For example, Cape Verde has its 2001 law publicly available in English, but we could not see the English version of the 2021 amended version; hence, it was excluded.

Furthermore, it is imperative to mention that few of the laws examined in this study were translated from another language. Therefore, some of the content may have been altered or mistranslated, which may have influenced our results. Benin, Côte d'Ivoire and Egypt are classic examples. Additionally, the choice of language of the law drafters was different and required reading more than once. Also, it is worth mentioning that only two of the three raters have legal backgrounds and are licensed to practise law in an African country.

Another limitation is that we only examined whether the law specifies establishing a data protection authority, whether each country has established one, and whether it is genuinely independent, which can be the focus of another study. Additionally, we limit ourselves to periodic compliance audits carried out by the data protection authorities and do not consider routine data protection impact assessments performed by the data controller or processor, which can also be examined in another study.

This study mainly examines enforcement mechanisms provided only by data protection laws. It serves as a bedrock for further research on the enforcement practices of African data protection authorities and their mode of operation in ensuring adherence to data protection laws following global best practices. Additionally, the effectiveness of civil sanctions and private right of action as an avenue for data subjects to seek remedy for data protection intrusions and the absence of class action mechanisms in African data protection laws examined can be the subject of a future study. It requires case law across Africa as empirical data to analyse it, just like Muhawe & Bashir examined the effect of Article III standing on private right of action in the United States using decided cases.[150]

Furthermore, this study aims to raise awareness of enforcement mechanisms in place in the selected African countries. It does not critically examine African cultural differences, external factors such as foreign direct investment and

150 Muhawe & Bashir (n 146).

international trade practices in the African technology sector, and their impact on enforcing data protection laws. Future studies can focus on these, especially with Nigeria imposing a US $220 million fine on Meta. Additionally, future work may examine the comparative analysis of the practical implications for local and foreign data controllers encountering various legislative frameworks with different compliance approaches and enforcement mechanisms and the encounters for transnational cooperation operating across Africa.

8 Conclusion

The promulgation of data protection laws in Africa has developed rapidly, making the continent a leading region in this area. Enforcement of data protection laws is the next phase of data privacy in Africa. As of March 2024, 38 out of 55 African countries had data protection laws, but other countries are making drastic efforts to enact these, such as Cameroon, Djibouti, Ethiopia and Namibia, which have pending data protection bills. Out of the 38 enacted African data protection laws, only 20 were publicly available in English.

The 20 data protection laws we examined apply to the public and private sectors, and about 55 per cent of the laws have extraterritorial effects, which make them binding to non-resident data controllers. Government-owned data protection authorities enforce, administer, and execute data protection laws in the 20 selected African countries. The data protection authorities were new independent agencies in 16 countries, while four other countries made existing government departments serve as data protection authorities. To ensure compliance, 50 percent of the examined countries empower the data protection authority to conduct periodic compliance audits.

Non-compliance with data protection laws attracts some sanctions. We observed that 85 per cent of the laws examined empower the data protection authorities to issue administrative sanctions such as notice of violation, cessation and penalty. All the countries examined provided for financial sanctions up to a specified amount or specified percentage of the data controller's annual return in the preceding financial year. Violators of data protection laws can be charged with a crime and sentenced to fines, imprisonment or forfeiture, and officers of the data controllers may be personally liable. Data subjects who suffered damage from violation of data protection laws can approach the court for compensation without usurping the power of the data protection authority in most of the countries we examined. However, data subjects in Tanzania are mandated to approach the data protection authority for financial compensation. Registration of data controllers with the data protection authorities is required in all the countries examined; the significant difference is the time of registration. For example, in South Africa, registration is required before processing personal data, while it is only required within six months of becoming a data controller of significant importance in Nigeria.

Further, most countries examined in this study prescribed an enforcement approach with some remarkable similarities with the EU GDPR, especially in creating data protection authorities and administrative, civil or financial sanctions that buttress the Brussels effect on enacting data protection laws worldwide. However, criminal sanctions still make a big difference in the data protection laws of the 20 selected African countries and the EU GDPR.

As stated earlier, the next stage of data privacy in Africa is enforcing data protection laws within and outside Africa. Since Africa is a leading region in the Global South with a youthful population and increasing internet users and, thus, this move can have a global impact and consequences not only for the region but also throughout the world. This type of enforcement could also provide African countries a massive source of revenue because about 55 per cent of countries examined in this study have extraterritorial reach provisions that make their laws applicable to data controllers and processors not domiciled in Africa but also around the world as it can shape cross-border enforcement. Illustratively, the imposition of a US $220 million fine on Meta by Nigeria will open a wider door of enforcement both locally in Africa and internationally. Therefore, we envision that data controllers and processors, especially big tech companies not based in Africa, will be paying serious attention to compliance with African data protection laws in the coming months and years as more African countries are taking drastic steps to ensure adherence to their data protection legislations and protect their citizens' data privacy, which will likely mould global data protection practices.

African Journal on Privacy & Data Protection

To cite: S Genga 'A review of the adequacy of Kenya's and South Africa's data protection legal frameworks in protecting persons with disabilities from artificial intelligence algorithm discrimination' (2025) 2 *African Journal on Privacy & Data Protection* 41-60
https://doi.org/10.29053/ajpdp.v2i1.0003

A review of the adequacy of Kenya's and South Africa's data protection legal frameworks in protecting persons with disabilities from artificial intelligence algorithm discrimination

*Shirley Genga**
Postdoctoral Research Fellow, Free State Centre for Human Rights, University of the Free State, Bloemfontein, South Africa

Abstract

As the use of artificial intelligence (AI) through automated decision making continues to increasingly influence decision making in various sectors, including employment, insurance, financial, health care and social services bringing efficiency, the likelihood of AI algorithm discrimination also grows. This discrimination is often perpetuated against vulnerable groups such as persons with disabilities (PWDs), who may already face significant societal barriers. This article delves into the question of whether Kenya's and South Africa's data protection laws adequately protect PWDs from AI algorithmic discrimination. The initial part of the paper explores how AI algorithms, when applied through automated decision making, can unintentionally lead to discrimination against PWDs. It does this by highlighting specific examples from various sectors,

* LLB LLM (Nairobi) PhD (Witwatersrand); Genga.SAA@ufs.ac.za or shirleyanngenga@yahoo.com

demonstrating how AI discrimination impacts on PWDs. The second part critically reviews the data protection legal framework in both Kenya and South Africa and, while providing a comparative analysis of both states, it focuses on their adequacy in protecting PWDs from AI discrimination. It does this in order to identify the strengths and limitations of both states' laws in protecting PWDs from algorithm discrimination. It will further provide recommendations for legal and policy reforms aimed at enhancing transparency, accountability and inclusivity in AI systems in both states in terms of regulating algorithmic discrimination of PWDs.

Key words: *artificial intelligence; discrimination; disability; data protection*

1 Introduction

It is estimated that 1,3 billion people experience disabilities, representing approximately one in six of the world's population.[1] These include a wide variety of disabilities, including visual, hearing, speech, mobility, cognitive and psychosocial.[2] Notably, persons with disabilities (PWDs) experience widespread stigma and discrimination.[3] They are often prevented from fully participating in society because of environmental and attitudinal barriers.[4] As a result, PWDs experience exclusion from education and employment, barriers in health systems and are at higher risks of experiencing poverty.[5]

Further, although, generally speaking, technology makes life convenient for most, for PWDs, technology provides independence.[6] Technology helps to remove barriers to participating in society. As a result of technology, PWDs can access education, health, transport, employment, leisure, culture, and participate in other areas of life never imagined previously.[7]

Importantly, when it comes to technology, no other area has impacted the lives of PWDs like the internet of things (IoT).[8] IoT refers to a 'network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share

1 WHO 'Disability: Key facts' 7 March 2023, https://www.who.int/news-room/fact-sheets/detail/disability-and-health (accessed 21 July 2024).
2 DS Raja (World Bank Group) 'Bridging the disability divide through digital technologies, world development report' (2016) 5, http://pubdocs.worldbank.org/en/123481461249337484/WDR16-BP-Bridging-the-Disability-Divide-through-Digital-Technology-RAJA.pdf, https://giwps.georgetown.edu/dei-resources/bridging-the-disability-divide-through-digital-technologies/ (accessed 21 July 2024).
3 WHO (n 1); C Marzin 'Plug and pray? A disability perspective on artificial intelligence, automated decision-making and emerging technologies' (2018) 5, https://www.edf-feph.org/content/uploads/2020/12/edf-emerging-tech-report-accessible.pdf, https://www.edf-feph.org/publications/plug-and-pray-2018/ (accessed 21 July 2024).
4 Marzin (n 3) 5.
5 WHO (n 1); Marzin (n 3) 5.
6 Marzin (n 3) 5.
7 As above.
8 As above.

data. IoT devices are also known as smart objects.'[9] These include everything from assistive devices, to wearables such as smart watches, to industrial machinery and transportation systems.[10] These IoT-connected assistive technologies are intentionally designed to assist PWDs in the different facets of their daily lives.[11] Indeed, many of today's IoT devices and services are specifically designed for PWDs, whereas others are repurposed by them.[12] For PWDs, the IoT can be transformational because it can enhance communication, socialising, safety, mobility in both physical and virtual environment.[13]

In addition, computers today can learn, and artificial intelligence (AI) is integrated into the products we use every day.[14]

AI has the potential to not only revolutionise the industrial sector, but also the quality of people's lives,[15] and this is what has influenced the participation of both private and public actors.[16] Therefore, there is no aspect of life today that is not been impacted by AI, including assistive devices for persons with disabilities.[17]

Significantly, while there is no agreement on the definition of AI, an essential element that has been identified is that it covers systems that think like humans or act like human beings.[18] AI technologies are 'typically based on algorithms that make predictions to support or even fully automate decision making'.[19] Algorithms 'process are a set of rules to be followed in calculations or other problem-solving operations, especially by a computer'.[20] Moreover, algorithms are used to automate a wide range of everyday tasks on a scale far beyond what

9 IBM 'What is the IoT?', https://www.ibm.com/topics/internet-of-things (accessed 30 July 2024).
10 As above.
11 A Habbal and others 'Privacy as a lifestyle: Empowering assistive technologies for people with disabilities, challenges and future directions' (2024) 36 *Journal of King Saud University – Computer and Information Sciences* 2.
12 Future of Privacy Forum 'The internet of things and people with disabilities: Exploring the benefits, challenges and privacy tensions' January 2019 1, https://fpf.org/wp-content/uploads/2019/01/2019_01_29-The_Internet_of_Things_and_Persons_with_Disabilities_For_Print_FINAL.pdf (accessed 21 July 2024).
13 As above; M Marks 'Algorithmic disability discrimination' in G Cohen & C Shachar (eds) *Disability, health, law, and bioethics* (2020) 243.
14 Marzin (n 3) 5.
15 E Ferrara 'Fairness and bias in artificial intelligence: A brief survey of sources, impacts, and mitigation strategies' (2024) 6 *Sci* 2.
16 M Buyl and others 'Tackling algorithmic disability discrimination in the hiring process: An ethical, legal and technical analysis' 2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22) 21-24 June 2022, Seoul 1.
17 As above.
18 AB Nougrères 'Report of the Special Rapporteur on the Right to Privacy: Principles of transparency and explainability in the processing of personal data in artificial intelligence' (30 August 2023) A/78/310 para 7; T Krupiy & M Scheinin 'Disability discrimination in the digital realm: How the ICRPD applies to artificial intelligence decision-making processes and helps in determining the state of international human rights law' (2023) 23 *Human Rights Law Review* 1, 2.
19 EU Agency for Fundamental Rights (FRA) 'Bias in algorithms – Artificial intelligence and discrimination' (2022) 7, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf (accessed 21 July 2024).
20 Marzin (n 3) 6.

humans can achieve.[21] They can analyse, infer, predict, label and recommend and, as a result, have opened up new horizons and can support decision making across many domains.[22] AI algorithms are the backbone of AI, enabling machines to replicate human-like intelligence and execute multifaceted tasks such as automated decision making (ADM).[23] ADM basically refers to using AI algorithms to make decisions without human involvement.[24]

Nowadays, ADM systems are used extensively throughout different industries across African countries, invading every sector including finance, education, health care, business and public administration, and both Kenya and South Africa have not been left behind.[25] In order to bolster accurate and efficient service delivery, these sectors are increasingly using ADM.[26] For example, in Kenya we have Felisa, a money-lending product; Tala, a credit service;[27] the Angaza Elimu, M-shule and iMlango system in the education sector;[28] and Boma Yangu portal, a government system to operationalise its affordable housing project.[29] In South Africa, examples include 'First National Bank's Manila platform using AI to flag fraud, money laundering, and tax evasion risks'; Daptio, an education platform;[30] and the Department of Education in Gauteng utilises a fully ADM system to ensure fair placement of students at schools and uses factors such as proximity to schools and other relevant factors in making these determinations.[31]

2 Use of AI algorithms in decision making and the risk of bias

AI systems are changing the lives of persons with disabilities at an amazing rate never previously imagined.[32] Nevertheless, the application of AI systems is not unproblematic and comes with its share of challenges.[33] Indeed, the trend that poses a series of risks for PWDs is the everyday use of AI algorithms for

21 FRA (n 19) 7.
22 As above.
23 M Viola de Azevedo Cunha 'Child privacy in the age of web 2.0 and 3.0: Challenges and opportunities for policy' UNICEF Innocenti Discussion Paper March 2017 10, https://cadmus.eui.eu/handle/1814/49884 (accessed 23 December 2024); Artificial Intelligence (AI) Algorithms (10 April 2024), https://www.geeksforgeeks.org/ai-algorithms (accessed 23 December 2024).
24 Centre of Intellectual Property and Technology Law (CIPIT) co-authored with LO Orero & J Kaaniru (Strathmore University) 'Policy brief – Automated decision-making policies in Africa' (2023) 3, https://cipit.strathmore.edu/category/publications/policy-briefs/ (accessed 23 December 2024).
25 Centre for Intellectual Property and Information Technology law(CIPIT) 'The applications, challenges and regulation of automated decision-making (ADM) in Africa' 8 November 2024 7, https://cipit.strathmore.edu/the-applications-challenges-and-regulation-of-automated-decision-making-adm-in-africa/ (accessed 30 December 2024).
26 As above.
27 CIPIT (n 24) 8.
28 CIPIT (n 24) 9.
29 As above.
30 As above.
31 As above.
32 Buyl and others (n 16) 1.
33 As above.

automated decision making (ADM) online.[34] They are exposed to 'pervasive surveillance, persistent evaluation, insistent influence, possible manipulation and discrimination'.[35] This article will specifically focus on the ability of ADM to discriminate against persons with disabilities.

The use of ADM is often depicted as rational and neutral, but this is not true because of human influence. They are developed and used by humans. As a result, if bias is present in human decision making, it can be replicated by machines.[36] Indeed, it is now an accepted fact that AI systems, ADM, can discriminate against some categories of the population.[37] This is especially true when privacy and other ethical standards are not implanted in algorithms, then their use can result in the discrimination of PWDs.[38] AI applications 'process personal data in two ways'. Primarily, personal data is the source material used to teach machine learning systems in order to build their algorithmic models.[39] Once built, the same models can be used to analyse and interpret personal data to make inferences concerning particular individuals.[40]

Interestingly enough, one of the reasons discrimination occurs is because algorithms are 'fuelled' or trained by personal data that is biased.[41] In fact, algorithms are biased when they learn or are trained by biased data.[42] If the data employed in the training of the machine learning models contains any bias, the analysis conducted by the algorithm will follow the same pattern and in some instances introduce new ones.[43] Bias refers to 'the systematic errors that occur in decision-making processes, leading to unfair outcomes'.[44] Hence, it can lead to AI discrimination based on disability if the bias is towards persons with disabilities. Significantly, apart from data used for training AI, other potential sources of bias include algorithm design and human interpretation.[45] AI discrimination is of crucial concern for persons with disabilities because the industries where ADM use is on the uptake in the same sectors where PWDs have historically encountered and continue to encounter barriers and exclusion. These include welfare benefits, employment opportunities and healthcare decisions.[46] If not

34 Viola de Azevedo Cunha (n 23) 10.
35 G Sartor (STOA) 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' (2020) ii, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (accessed 21 July 2024).
36 FRA (n 19).
37 Marzin (n 3) 25.
38 Viola de Azevedo Cunha (n 23) 10.
39 Sartor (n 35).
40 As above.
41 Marks (n 13) 243.
42 Marzin (n 3) 26.
43 Sartor (n 35) i; Marks (n 13) 243.
44 Ferrara (n 15) 2.
45 Ferrara (n 15) 4.
46 G Alexiou 'Disability data alarmingly absent from AI algorithmic tools, report suggests' 6 August 2024, https://www.forbes.com/sites/gusalexiou/2024/08/06/disability-data-alarmingly-absent-from-ai-algorithmic-tools-report-suggests/ (accessed 25 December 2024).

adequately regulated, the use of ADM can perpetuate and even magnify already-existing inequalities.

2.1 AI discrimination based on disability

Kenya and South Africa have ratified the United Nations (UN) Convention on the Rights of Persons with Disabilities (CRPD).[47] Additionally, CRPD assumes a social understanding of disability when it comes to defining disability. This is important because it highlights a change from the medical model of disability, which is the historically-dominant model whose focus is on correcting or curing the individual to fit society.[48] Contrastingly, a social understanding of disability highlights the fact that disability is created when the social environment fails to change to meet the needs of individuals with impairments.[49] Further, because a social model of disability infers that a comprehensive approach is adopted in disability anti-discrimination law, CRPD recognises all the different types of discrimination, which include 'direct and indirect discrimination, harassment and the denial of reasonable accommodation';[50] also, recognising discrimination by association, and multiple and intersectional discrimination.[51]

To discriminate on an elemental level means to differentiate.[52] CRPD defines discrimination on the basis of disability as

> any distinction, exclusion or restriction on the basis of disability which has the purpose or effect of impairing or nullifying the recognition, enjoyment or exercise, on an equal basis with others, of all human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field. It includes all forms of discrimination, including denial of reasonable accommodation.[53]

Accordingly, an AI algorithm theoretically discriminates against a person with a disability whenever it makes an automated decision based on their disability that excludes or restricts that and that leads to disparate impact, unjustifiable disadvantage.[54] Lastly, the differentiation need not be intentional.[55] Kenyan law

47 United Nations Human Rights Treaty Bodies, Ratification Status for CRPD – Convention on the Rights of Persons with Disabilities, https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?Treaty=CRPD (accessed 21 July 2024).

48 SA Genga 'Legal responses to employment discrimination on the basis of psychosocial disabilities: Kenya's and South Africa's compliance with the Convention on the Rights of Persons with Disabilities' unpublished PHD thesis, University of the Witwatersrand, 2021 71, 25.

49 Genga (n 48) 71.

50 Genga (n 48) 51, 184-193.

51 Genga (n 48) 71, 184-193.

52 JL Roberts 'Protecting privacy to prevent discrimination' (2015) 56 *William & Mary Law Review* 2109.

53 Art 2 Convention on the Rights of Persons with Disabilities.

54 H Weerts and others 'Unlawful proxy discrimination: A framework for challenging inherently discriminatory algorithms' (2024) ACM Conference on Fairness, Accountability, and Transparency (FAccT '24) 3-6 June 2024, Rio de Janeiro, Brazil, ACM, New York, NY, USA, https://doi.org/10.1145/3630106. 3659010, 1850; Roberts (n 52) 2109.

55 Roberts (n 52) 2109.

and South African law both recognise all forms of discrimination recognised by CRPD.[56] This widens the reach and scope of anti-discrimination in both countries and, hence, for example, sets the ground to claim intersectional AI discrimination based on disability.

2.2 Examples of AI discrimination based on disability

There are a number of ways in which AI algorithm discrimination (AI discrimination) can occur. To begin with, when one engages in an image search for 'athlete' or even of a 'beautiful girl' on today's AI-enabled internet search engines, they are unlikely to yield images of athletes with disabilities or a girl with a physical disability. This is fuelled by the fact that the internet search engines rely on a data set or algorithm that holds to the outdated belief that persons with disabilities cannot be athletes,[57] or even beautiful.

Second, AI discrimination can also occur through targeted online advertising. For example, companies such as Meta and Google rely on targeted advertising.[58] Targeted online advertising relying on ADM can lead to the discrimination of PWDs.

An example is if a person has an eating disorder such as bulimia (which falls into the category of psychiatric or psychosocial disability). Discrimination can occur where a consumer with anorexia is profiled based on their data and is served customised advertisements selling weight loss products as a result.[59] This type of marketing is exploitative and is called 'vulnerability-based marketing'.[60] Another example of targeted advertising is when algorithms infer one's disability from one's personal data. For example, an AI algorithm through one's digital footprint can identify that a person has a visual disability through their use of a screen reader or a braille keyboard even when they may not have publicly disclosed their disability. This information can be used to push advertisements for assistive devices used by persons with visual disabilities and other products.[61] Additionally, this information can also be used to deny or increase insurance coverage, or to exclude a person with disability from receiving ads for employment, education, housing and other resources, and hence exclude them from fully participating in society.[62]

56 Genga (n 48) 111-118, 140-152.
57 Rights of persons with disabilities, Report of the Special Rapporteur on the Rights of Persons with Disabilities (28 December 2021) UN DOC A/HRC/49/52 para 61.
58 FJZ Borgesius 'Strengthening legal protection against discrimination by algorithms and artificial intelligence' (2020) 24 *International Journal of Human rights* 1575; Marks (n 13) 244.
59 Marks (n 13) 244.
60 As above.
61 Marks (n 13) 243.
62 As above; Marzin (n 3) 25.

Also, AI based discrimination can occur if an organisation uses an AI recruitment system that has been trained on data from past human decisions that discriminated against persons with disabilities. A real-life example is when Amazon was forced to stop the use of an automated recruitment tool that was found to be biased against women.[63] The automated recruitment algorithm was trained on *curricula vitae* sent to Amazon over a period of ten years. A majority of the *curricula vitae* came from men, and hence the recruitment algorithm showed a preference for applications by men and rejected applications by women.[64]

Another example is when AI proxy discrimination occurs. This is when an outwardly neutral feature or variable (proxy attribute) that is associated or correlated with a specific protected ground is used as the ground for making a decision, leading to disparate impact.[65] However, at first glance it may seem that a person was denied an opportunity based on a facially-neutral feature, and so no discrimination occurred, but upon close inspection the connection between the facially-neutral feature, proxy attribute, can be made with the protected ground, hence highlighting that discrimination occurred.[66] For example, in a state where its provinces are predominantly inhabited by certain ethnic groups, postal codes may indirectly indicate a person's ethnicity. Here the 'postal code can be a proxy for ethnicity', and hence an ADM that makes a decision to accept or reject a job application based on one's postal codes could be held liable for engaging in ethnic proxy discrimination if the result leads to a disparate impact.[67] AI systems may unintentionally have discriminatory effects.[68]

A recent case example of proxy discrimination based on disability is the American case of *Mobley v Workday, Inc*.[69] Here Derek Mobley brought an action for employment discrimination against Workday, which provides employment screening services.[70] Mobley claimed that Workday's ADM application screening tool discriminated against him based on race, age and disability.[71] According to Mobley, he had been overlooked for numerous job opportunities at other companies that also contracted 'with Workday because he is black, over 40 and has anxiety and depression'.[72] Further, he claimed that Workday's algorithms could infer personal details about him, such as his age, race and background,

63 Marzin (n 3) 26.
64 As above.
65 Weerts and others (n 54) 1850.
66 M van Bekkum & FZ Borgesius 'Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?' (2023) 48 *Computer Law and Security Review* 3; Weerts and others (n 54) 1851-1852.
67 Weerts and others (n 54) 1852.
68 Van Bekkum & Borgesius (n 66).
69 Case 23-cv-00770-RFL, FindLaw, https://caselaw.findlaw.com/court/us-dis-crt-n-d-cal/116378658.html?utm_source=chatgpt.com; D Wiessner 'Workday must face novel bias lawsuit over AI screening software' 16 July 2024, https://www.reuters.com/legal/litigation/workday-must-face-novel-bias-lawsuit-over-ai-screening-software-2024-07-15/ (accessed 29 December 2024).
70 As above.
71 As above.
72 Wiessner (n 69).

based on other information. These include information on when he graduated, the schools he attended (including his degree from a historically black college). Also, the numerous positions for which he applied 'required him to take a Workday-branded assessment and/or personality test, and to provide other personal information from which his disability could be inferred'.[73] He argued that the use of the ADM tool infringed on anti-discrimination law.[74] On 15 July 2024 a bid to dismiss the class action was rejected.[75]

As of yet, there are no available cases in either state, but as has been highlighted, both states are using ADM in different industries,[76] and so it is only a matter of time. Other American cases include *Louis & Others v SafeRent Solutions & Others*;[77] *Equal Employment Opportunity Commission v iTutorGroup, Inc*;[78] and *KW ex rel DW v Armstrong*.[79]

3 Data protection legal framework and AI discrimination regulation

As it stands in both Kenya and South Africa, anti-discrimination law and data protection law are the main tools for protecting persons with disabilities against AI discrimination. Notably, Kenya currently has an AI Bill that has been drafted, but which has not yet been passed into law by Parliament.[80] This research will mainly focus on data protection laws in both states as AI algorithm anti-discrimination tools. Nevertheless, it is worth noting that as an anti-discrimination tool, data protection law remains largely untested generally,[81] and the legal frameworks in both states are no different.

This article chose to focus on both Kenya's and South Africa's legal frameworks as both are developing African states that have passed comprehensive data

73 FindLaw, https://caselaw.findlaw.com/court/us-dis-crt-n-d-cal/116378658.html?utm_source=chatgpt.com (accessed 21 July 2024); Wiessner (n 69).
74 As above.
75 Wiessner (n 69).
76 CIPIT (n 25) 7-9.
77 1:22-cv-10800, C Milstein, https://www.cohenmilstein.com/case-study/louis-et-al-v-saferent-solutions-et-al/ (accessed 29 December 2024).
78 1:22-cv-02565, (EDNY), https://www.workforcebulletin.com/assets/htmldocuments/blog/8/2023/08/2023.08.09-EEOC-v.-iTutorGroup-Joint-Notice-of-Settlement-22-cv-02565-PKC-PK.pdf; Court Listener, https://www.courtlistener.com/docket/63288748/equal-employment-opportunity-commission-v-itutorgroup-inc/#:~:text=Opportunity%20Commission%20v.-,iTutorGroup%2C%20Inc.,%3A22%2Dcv%2D02565) (accessed 23 December 2024).
79 789 F.3d 962 (9th Cir 2015); G van Toorn (ARC Centre of Excellence for Automated Decision-Making and Society and Data Justice Lab) 'United against algorithms: A primer on disability-led struggles against algorithmic injustice' 15 April 2024, https://apo.org.au/node/326312 19 (accessed 21 July 2024); E McCormick 'What happened when a "wildly irrational" algorithm made crucial healthcare decisions' 2 July 2021, https://www.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions (accessed 21 July 2024).
80 The Kenya Robotics and Artificial Intelligence Society Bill, 2023, https://www.dataguidance.com/sites/default/files/the_kenya_robotics_and_artificial_intelligence_society_bill_2023.docx.pdf (accessed 21 July 2024).
81 Borgesius (n 58) 1582.

protection laws whose provisions are currently in force. Further, both states have a data protection commissioner's office that is operational and established by law to supervise and enforce data protection law in both states.[82] Data protection law safeguards the rights of data subjects and establishes corresponding responsibilities for data processors and controllers who collect the data.[83] Although the purpose of data protection law is to protect personal information, to that end, it can also be used to protect other standards and rights, in this instance, anti-discrimination rights in the use of AI. Correspondingly, Marvin and Frederik state that apart from data privacy, data protection law can also be used for anti-discrimination purposes and to protect other rights.[84]

However, it is crucial to note that a tension exists between AI and traditional data protection principles.[85] Nevertheless, data protection principles can be translated and applied in a way that aligns with the advantageous application and use of AI.[86] The principles and provisions can be interpreted and understood in a way that is consistent with and beneficial to the application of AI, as will be highlighted.[87]

Further, in order to identify the adequacy of the legal frameworks of both states in protecting PWDs from AI discrimination, this article will put up two arguments.

To begin with, Roberts and Schwarcz argue that protecting privacy can limit discrimination. This is done when data protection law limits access to the very information discriminators use to discriminate.[88] Limiting access acts as a barricade against detrimental differentiation.[89]

Roberts argues that unlawful discrimination frequently requires discriminators to be informed about protected status.[90] For instance, in the context of employment,

82 Office of the Data Protection Commissioner (ODPC) 'Data commissioner inaugurates for data protection officers on data protection impact assessment' 24 April 2024, https://www.odpc.go.ke/data-commissioner-inaugurates-training-for-data-protection/ (accessed 30 December 2024); The Information Regulator (South Africa) 'Members of the Information Regulator', https://inforegulator.org.za/members-2/ (accessed 30 December 2024).

83 Borgesius (n 58) 1576.

84 Van Bekkum & Borgesius (n 66) 5; A Calvi 'Exploring the synergies between non-discrimination and data protection: What role for EU data protection law to address intersectional discrimination?' (2023) 14 *European Journal of Law and Technology*; D le Métayer & J le Clainche 'From the protection of data to the protection of individuals: Extending the application of non-discrimination principles' in S Gutwirth and others (eds) *European data protection: In good health? (*2012) 315- 316.

85 Sartor (n 35) ii.

86 Sartor (n 35) i.

87 Sartor (n 35) ii.

88 Roberts (n 52) 2097; D Schwarcz 'Health-based proxy discrimination, artificial intelligence, and big data' (2021) *Houston Journal of Health Law and Policy* 4; MC Tschantz 'What is proxy discrimination?' (2022) ACM Conference on Fairness, Accountability, and Transparency (FAccT '22) 1, 21-24 June 2022, Seoul, Republic of Korea. ACM, New York, NY, USA, https://doi.org/10.1145/3531146.3533242 (accessed 21 July 2024).

89 Roberts (n 52) 2101.

90 Roberts (n 52) 2097.

an employer cannot discriminate against an employee based on disability or any other protected characteristic if they do not have access to that information.[91] In actuality, it would be difficult and even impossible for an employer to consciously or unconsciously ground their decision on an employee based on their disability or another protected ground if the employer does not know about the employee's disability or other protected ground.[92] Hence, restricting the access of potential discriminators from information about one's protected status can significantly reduce the chances of subsequent discrimination.[93] In accordance with this, this article makes the argument that when data privacy law limits the processing of disability data, it also protects persons with disability from AI discrimination. In addition, the article builds on this argument by Roberts and adds that disability data should not just be protected as personal data in general, but adds that disability data should be protected as a sensitive class of data requiring a greater level of protection. Generally, special or sensitive data is not allowed to be processed except in exceptional circumstances. Data that falls under this category requires more protection because of its sensitive nature.[94]

This article argues that there are a number of reasons why disability data should automatically fall in the category of special or sensitive data.

Primarily, this is because PWDs are often vulnerable and heavily discriminated against generally.[95] The very knowledge of a person's disability is sensitive as it can expose the said person to discrimination, and that is why the privacy protection of a person's disability status can often lead to their protection from discrimination.

Additionally, although emerging technologies, especially assistive devices, are key to elevating the quality of life for PWDs by facilitating their participation in society, the same technology puts their privacy at risk.[96] This is because assistive devices also collect and process sensitive data.[97] Further, it is not only the assistive devices, but persons with disabilities are also exposed to the collection of personal information in the workplace. For example, this occurs when a PWD requests to be reasonably accommodated or when they seek social services or health care. Further, it is not just assistive devices or the workplaces, but it almost seems as if to access and participate in society, persons with disabilities are constantly put in positions where they must share detailed sensitive information. In public spaces they are constantly attempting to balance the need for accessibility with the

91 Roberts (n 52) 2099.
92 As above.
93 Roberts (n 52) 2099-2100.
94 UK information Commissioner's Office 'Special category data', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/special-category-data (accessed 29 December 2024).
95 WHO (n 1).
96 Habbal and others (n 11) 2.
97 As above.

desire to protect their privacy.[98] Therefore, privacy is a key concern for persons with disabilities because a big chunk of their lives is managing privacy in order to have access to participation in society.[99] Consequently, for data protection to be effective in protecting PWDs from AI discrimination, disability data should be protected as special or sensitive data.

The second argument that the article makes is that while preventing access to the processing disability data as special or sensitive data is key to providing protection against AI discrimination, it is not sufficient, and that the same law should also allow for specific circumstances where the same disability data should be processed for anti-discrimination purposes.[100] Therefore, the same law that limits the processing of data that falls into the category of special or sensitive data, in this case, disability data, will additionally need to provide specific and limited exceptions for processing of the said data for auditing or debiasing purposes.[101] For instance, if a company utilising an ADM system to select the best candidate wants to determine whether its AI system discriminates against individuals with disabilities or any other protected characteristic, such as ethnicity, it must conduct an audit. In order to conduct such an audit, the company requires access to data on applicants' disabilities or ethnicities.[102]

Consequently, although strict rules on special or sensitive categories of data limit discrimination on one end, a strict regime also acts as a barrier when it comes to assessing and mitigating discrimination.[103] Furthermore, the allowance to process disability data for auditing and debiasing purposes is particularly crucial for PWDs because although the use of ADM tools is growing in popularity globally, a 2024 report by the Centre for Democracy and Technology has found that there is inadequate high-quality data about persons with disabilities.[104]

This allowance to process disability data for debiasing or auditing purposes, in my view, captures the spirit of the principles of transparency and explainability which, according to a report by the UN Special Rapporteur on the Right to

98 L McRae and others Privacy and the ethics of disability research: Changing perceptions of privacy and smartphone use' in J Hunsinger and others (eds*) Second international handbook of internet research* (2020) 413.

99 As above.

100 T Marwala 'The dual faces of algorithmic bias – Avoidable and unavoidable discrimination' 30 January 2024, https://www.dailymaverick.co.za/opinionista/2024-01-30-the-dual-faces-of-algorithmic-bias-avoidable-and-unavoidable-discrimination/ (accessed 30 January 2024); CIPIT (n 25) 14; RJ Chen and others 'Algorithmic fairness in artificial intelligence for medicine and healthcare' (2023) 7) *Nature Biomedical Engineering* 719-742, 6 and 47; Weerts and others (n 54)1852.

101 As above; Van Bekkum & Borgesius (n 66) 5; Rights of persons with disabilities, Report of the Special Rapporteur on the Rights of Persons with Disabilities (28 December 2021) UN DOC A/HRC/49/52 para 62; Tschantz (n 88) 1.

102 Borgesius (n 58) 1579.

103 Borgesius (n 58) 1581.

104 A Aboulafia and others (Centre for Democracy and Technology) Report – To reduce disability bias in technology, start with disability data 25 July 2024 6-7, https://cdt.org/wp-content/uploads/2024/07/2024-07-23-Data-Disability-report-final.pdf (accessed 21 July 2024); Alexiou (n 46).

Privacy, are significant for the reliable use of AI.[105] This is because AI systems suffer the challenge of being opaque, in that it is a challenge for users to understand how it works.[106] Its opaqueness magnifies the inability to recognise and 'prove possible breaches of laws, including legal provisions that protect fundamental rights, attribute liability and meet the conditions to claim compensation'.[107] This is why transparency and explainability are key principles; they require that the use of AI and ADM should also be accompanied by information that explains the process of how the decision was made.[108]

According to the Special Rapporteur's report, the potential opacity of AI may be alleviated by mandating adherence to minimum transparency standards.[109] The principle of transparency requires that 'when interacting with an AI system and not a human being, users should be clearly informed in an objective, concise and easily understandable way'.[110] Explainability, on the other hand, requires that with every decision an in-depth explanation should be provided, especially when the decision 'impacts the end user in a way that is not temporary, easily reversible or otherwise low risk'.[111] Additionally, a data subject should be informed about the reasoning behind the decision and the specific data that was utilised. This information is crucial as it allows the data subject to determine whether the decision was correct and, if not, it provides them with relevant evidence to defend themselves or make a claim in a court of law in case of inaccuracies or an injustice such as AI discrimination.[112] Transparency and explainability are key in building trust in the use of AI.[113] Hence, this article reviews the data protection laws in both Kenya and South Africa to identify whether both entrench the principles of transparency and explainability as an AI anti-discrimination tool.

3.1 Kenya's data protection law and AI discrimination

The Kenya Data Protection Act 2019 (KDPA) was adopted by the National Assembly and assented to by the President of Kenya on 8 November 2019.[114] The law 'came into force on 25 November 2019 and gives effect to articles 31(c) and (d) of the Constitution of Kenya, 2010'.[115]

105 Nougrères (n 18) para 1.
106 A Facchini & A Termine 'Towards a taxonomy for the opacity of AI systems' in VC Muller (ed) *Philosophy and theory of artificial intelligence* (2021) 73.
107 Para 27.
108 AM Laibuta 'Adequacy of data protection Regulation in Kenya' unpublished PhD thesis, University of the Witwatersrand, 2023 171.
109 Nougrères (n 18) para 28.
110 As above.
111 Nougrères (n 18) para 31.
112 Nougrères (n 18) para 50.
113 Nougrères (n 18) para 63(a).
114 Amnesty International Kenya 'Comparative study on data protection regimes' (2021) 11, https://restoredatarights.africa/wp-content/uploads/2021/12/Amnesty-International-Kenya-Data-Protection-Report-Pages-1.pdf (accessed 21 July 2024).
115 As above.

It provides guidance on the collection, storage, processing, dissemination and transfer of personal data in Kenya. Additionally, it provides legal recourse where there is misuse or abuse of personal data.[116] The first data protection commissioner is Ms Immaculate Kassait, who assumed office on 16 November 2020,[117] and to date remains in office.[118]

To start with, the Act fails to specifically define disability data as special or sensitive data. The KDPA states that personal data is 'any information relating to an identified or identifiable natural person'.[119] This includes the processing of disability data covered. The Act further outlines a category of personal data that requires greater protection under the banner of sensitive data. The Act in section 2 defines sensitive personal data and does not mention disability data as belonging to the category under the Act.[120] However, one could make the case that disability data falls under the category of health data, which is mentioned as belonging to the sensitive personal data category. Nonetheless, the Act defines health data as

> data related to the state of physical or mental health of the data subject and includes records regarding the past, present or future state of the health, data collected in the course of registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.[121]

Looking at the definition, it can be argued that there may be instances where disability data could qualify as health data according to the definition, which seems to include the aspect of disability data that is captured when a person with disability seeks health care service. Nonetheless, this is limiting because it does not, for example, include disability data that is collected for social services, employment, or while using assistive devices or for other purposes or reasons.

Further, although health conditions and problems sometimes cause disability, health and disability are two distinct categories.[122] This is because a person can have a disability and be healthy. As well, studies consistently report substantial health disparities and experiences among persons with disabilities.[123] For example, some individuals with disabilities are born with conditions such as blindness or show signs of a disabling condition early in life. Others may acquire a disability

116 Kenya Data Protection Act 24 of 2019.
117 Amnesty International Kenya (n 114) 11; Laibuta (n 108) 172.
118 Office of the Data Protection Commissioner (ODPC) 'Data commissioner inaugurates for data protection officers on data protection impact assessment' 24 April 2024, https://www.odpc.go.ke/data-commissioner-inaugurates-training-for-data-protection/ (accessed 30 July 2024).
119 Kenya Data Protection Act 24 of 2019 sec 2.
120 As above.
121 As above.
122 S Yee & M Lou Breslin 'Disability rights education and Defence Fund: This data, not that data: Big data, privacy, and the impact on people with disabilities' (March 2023) 1, https://healthlaw.org/wp-content/uploads/2023/03/This-Data-Not-That-Data_Disability-Rights-Education-and-Defense-Fund_FINAL.pdf (accessed 21 July 2024).
123 As above.

later, such as through a spinal cord injury. Additionally, some people develop disabilities later in life, such as dementia or age-related mobility challenges.[124] As a result, health needs vary depending on the type and the cause of one's disability.[125] Thus, for some, the nature of their disability can be easily differentiated from their health status, for example, a person who is born blind. Alternatively, for others, their health status may directly lead to their disability, for example, the loss of a limb as a result of diabetes.[126]

The Act's definition of health data does not adequately capture the different complexities of disability data. As a result, it is possible that some disability data, for example, disability data collected for social services, government services or collected by assistive tools, is open for collecting and processing and will not be protected as special or sensitive data. Significantly, the American Data Privacy and Protection Act goes a step ahead of the KDPA and explicitly provides that sensitive data includes disability data.[127] This provides clarity and, importantly, recognises the fact that disability data also requires heightened protection, unlike the KDPA. This position by the KDPA limits the protection of PWDs from AI discrimination. Notably, though, the Act gives the data protection commissioner the authority to recommend additional types of personal data that could be grouped as sensitive personal data.[128] The commissioner has not as yet exercised these powers.

The Act, however, does allow exceptions for processing of disability data for auditing or debiasing purposes. According to KDPA, data controllers and processors have access to process disability data, which does not qualify as sensitive personal data in line with principles and requirements found in sections 25 to 43 of the Act. This includes disability data that does not qualify as data for health purposes as provided in section 30 of the Act. The Act also outlines exceptions in section 45 that allow for the processing of disability data, which may qualify as sensitive personal data. In fact, it can be argued that section 45(c) of the Act provides an avenue through which data controllers and processors can seek permission to process sensitive personal data for debiasing and auditing purposes with the aim of fighting AI discrimination, but this is not a given as it is not included as a specific exception.

Additionally, although the KDPA does not specifically mention AI, it does refer to ADM in section 35 of the Act. It provides that 'where a data controller or data processor takes a decision which produces legal effects or significantly affects

124 GL Krahn and others 'Persons with disabilities as an unrecognized health disparity population' (2015) *American Journal of Public Health* 198.
125 As above.
126 As above.
127 H.R.8152 – American Data Privacy and Protection Act, 117th Congress (2021-2022) sec 28(i), https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H0299B60817D742978DC3C447CD110A88 (accessed 29 July 2024).
128 KPDA sec 47; Amnesty International Kenya (n 114) 26.

the data subject based solely on automated processing, the data controller or data processor must, as soon as reasonably practicable, notify the data subject'.[129]

An organisation must inform a data subject when it uses ADM, but this does not specifically obligate the organisation to disclose information about the underlying reasoning of that decision-making process. The data processor or controller is not obligated to provide a clear and precise explanation about the solely automated decision. In fact, the only recourse for a data subject who experiences a legal effect as a result on ADM processes, in this case AI discrimination, is found in section 35(b) of the KDPA. It states that after a reasonable period has passed, the data subject has the authority to demand that the data controller or data processor reassess the ADM decision.[130] Another option is to request the data processor not to make a new decision solely based on ADM.[131] In response, a data controller or data processor is obligated to consider the request within a reasonable period[132] and to comply.[133] Further, the data subject should be informed of compliance with the request through a notice in writing.[134] Importantly, the Act is also silent on how a reasonable period will be determined under section 35. Here again, the Act blatantly fails to capture the transparency and explainability principle and limits the process of debiasing or auditing of the possible disability AI discriminatory process.

It is worth noting that according to section 35, 'every data subject has a right not to be subjected to a decision based "solely" on automated processing, including profiling'.[135] The word 'solely' is different from that provided in section 22 of the European Union (EU) General Data Protection Regulation (GDPR) which in article 22, referring to ADM, provides that it applies to decisions that are 'largely', rather than 'solely', like section 35 above. This leaves this section open to different interpretations. In fact, it could be argued that section 22 does not apply if a university denies a student admission based on a recommendation by an ADM system.[136] On the other hand, looking at Kenyan law, the question that arises is whether the law applies in instances where decisions are partly automated, which involves humans making decisions assisted by algorithms, for example, if an employer decides to hire an employee with a disability after an algorithmic system assessess the potential employee's qualifications.[137] Whether the Kenyan approach or EU approach is limited or effective is left to be seen. Nevertheless, a more effective approach would be to provide that the principle of transparency and explainability applies when the decision is both 'largely', 'partly'

129 Sec 35(3)(a).
130 Sec 35(3)(b)(i).
131 Sec 35(3)(b)(ii).
132 Sec 35(4)(a).
133 Sec 35(4)(b).
134 Secs 35(b) & (c).
135 Sec 35(1).
136 Borgesius (58) 1580.
137 Borgesius (58) 1573.

or 'solely' ADM. As long as AI processes are implemented, then, transparency and explainability should apply.

In addition, the data subject will not be alerted of an ADM process involving their data in a number of situations, namely, if the ADM

> is necessary for entering into, or performing, a contract between the data subject and a data controller or it is authorised by a law to which the data controller is subject, and which lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests; or is based on the data subject's consent.[138]

The Act then grants the cabinet secretary the power to create regulations and make further provisions to enhance the protection of the rights of the data subject when decisions are made solely by ADM process.[139] Notably, the adequacy of the relevant provisions of the KDPA, sections 2, 30, 45 and 35, have not yet been put to test in a court of law and, hence, their adequacy is difficult to determine, but from the review, it is clear that it is limited.

3.2 South Africa's data protection law and AI discrimination

The right to privacy is a fundamental right that is protected in the Constitution of South Africa.[140] Markedly, 'the Protection of Personal Information Act 4 of 2013 (POPIA) came into effect on 1 July 2020'. It was, however, 'subject to a one-year grace period, which ended on 30 June 2021'.[141] The South African POPIA adopts important features from global privacy laws and is considered to meet the protection standards outlined by the EU Directive.[142] Also, apart from providing data protection for only natural persons, POPIA also extends protection to legal persons.[143]

POPIA regulates the handling of personal data in South Africa, including the collection, storage, recording, retrieval, organisation, storage, alteration, use, updating, and distribution of personal information.[144]

138 Secs 35(2)(a), (b) & (c).
139 Sec 35(5).
140 Sec 14 of the Constitution; DLA Piper 'Data protection laws of the world: South Africa vs United Kingdom' (12 June 2024) 2, https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=ZA&country-2=GB (accessed 23 July 2024).
141 Constitution of the Republic of South Africa, 1996 sec 14; PJ de Waal 'The Protection of Personal Information Act (POPIA) and the Promotion of Access to Information Act (PAIA): It is time to take note' (2022) 35 *Current Allergy and Clinical Immunology* 232.
142 N Baloyi & P Kotzé 'Are organisations in South Africa ready to comply with personal data protection or privacy legislation and regulations?' IST-Africa 2017 Conference Proceedings, P Cunningham & M Cunningham (eds) IIMC International Information Management Corporation (2017) 2; A da Veiga & J Ophoff 'Concern for information privacy: A cross-nation study of the United Kingdom and South Africa' 14th International Symposium on Human Aspects of Information Security and Assurance (HAISA), July 2020, Mytilene, Lesbos, Greece 5.
143 Baloyi and Kotzé (n 142) 2.
144 Protection of Personal Information Act 4 of 2013 sec 1; S Mahomed and others 'The role of data transfer agreements in ethically managing data sharing for research in South Africa' (2022) 15 *South African Journal of Bioethics Law* 27.

Similar to Kenya, POPIA in section 26 prohibits 'the processing of special personal information'.[145] Nevertheless, unlike Kenya, POPIA in section 1 specifically lists disability data as falling into the category of personal information.[146] As a result, although POPIA provides that personal information relating to health falls into the category of special personal information and, hence, it is excluded from processing by section 26,[147] unlike Kenya, where disability data connected to health information could in some instances be considered special personal information, the same may not apply under this Act. This is because the Act specifically defines disability data as falling into the category of personal information.[148] As a consequence, the Act limits the protection of persons with disabilities from AI discrimination.

Additionally, section 71 of POPIA deals with ADM. Section 71(1) states that a data subject, in this case a person with a disability,

> may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its creditworthiness, reliability, location, health, personal preferences or conduct.[149]

Interestingly, unlike Kenya, although it prohibits the making of decisions concerning data subjects based entirely on an ADM process, it does not bind data processors or controllers with the obligation to notify the affected party when such a process or decision is undertaken. The principles of transparency and explainability demand that an affected party should always be notified. This limits the application of this section. On the other hand, although it does not have a notification obligation, it is more progressive than Kenyan law in that it provides that data processors or controllers, when notified by a data subject, in this case a PWD, with regard to a decision with legal consequences that was made solely on the basis of ADM, the data controller or processor is obligated to give the data subject information explaining the logic behind the decision or process.[150] Hence, an organisation can be obligated to explain that it used ADM and must provide relevant information on the foundational logic of that decision-making process.

However, in the same vein as Kenya, there are exceptions where data processors and controllers are not obligated to provide the data subject with adequate information on the foundational logic behind the ADM process in a number of situations in section 71(2) of POPIA.

145 Sec 26 POPI.
146 Sec 1 POPI, definition of special personal information.
147 Sec 26(a)(1) POPIA.
148 Sec 1(c) POPIA, definition of special personal information.
149 Sec 71(1) POPIA.
150 Sec 71(3)(b).

Correspondingly to Kenya, the relevant provisions on AI discrimination have been discussed. Sections 71 and 26 have not yet been put to test in a court of law. Nonetheless, based on this review, it is limited in protecting persons with disabilities from AI discrimination. This is because, as has been highlighted, POPIA does not categorise disability data as special data and, hence, denies this data a greater level of protection. Second, although it may be argued that section 71 of POPIA is more progressive than section 35 of Kenya's KDPA in that it obligates the data processor and controller to provide relevant information in the case of using solely automated processing, it fails to accurately capture the principles of transparency and explainability in that it does not obligate the same data processor and controllers to notify data subjects of it use. Therefore, one is left wondering how a data subject, in this case a PWD, will be able to identify when a solely automated process has been used with regard to their data.

4 Conclusion

In summary, while emerging technologies such as AI come with great benefits that increase the inclusion and participation of PWDs, it also comes with legitimate concern around AI disability discrimination.[151] Further, as has been highlighted, AI has brought many benefits, including independence, which is key for PWDs when it comes to fully benefiting from and participating in society. Thus, the solution lies in finding a balance between use of and access to the benefits of AI by PWDs, on the one hand, and anti-discrimination protection, on the other, from AI processes. As has been highlighted, both the Kenyan and South African laws have made progress when it comes to providing a law that can be used to regulate AI discrimination. Nevertheless, more needs to be done to ensure adequate protection of PWDs from AI discrimination. Both laws need to define disability data as falling within the category of special or sensitive data. Moreover, both laws need to explicitly or tacitly capture the principles of transparency and explainability in the sections that regulate AI processes. This will enable PWDs to be adequately protected from AI discrimination.[152] Nonetheless, transparency and explainability is not always practical or even attainable because of the opaqueness associated with algorithmic decisions, which makes it difficult to explain.[153] It is not always easy to clearly explain the logic behind a decision and, in some circumstances, an explanation might not be helpful.[154] While data protection laws play a crucial role in safeguarding persons with disabilities against AI discrimination, a significant part of the solution lies in technical advancements. This involves redesigning algorithms or developing

151 V Cobigo & K Czechowski 'Protecting the privacy of technology users who have cognitive disabilities: Identifying areas for improvement and targets for change' (2020) 7 *Journal of Rehabilitation and Assistive Technologies Engineering* 1; Marzin (n 4) 4.
152 Nougrères (n 18) para 64(b).
153 MF Nkonge 'Legal challenges facing algorithmic decision-making in Kenya' (2022) *University of Nairobi Law Review* 18; Nougrères (n 18) para 57.
154 Borgesius (n 58) 1581.

alternative versions that align with ethical standards and regulatory requirements, wherever feasible.[155] There is a need to advance algorithmic systems that facilitate transparency and explainability.[156] Lastly, it may be too early to assess the effects of data protection law can have on AI discrimination in both states as more legal research and jurisprudential development is needed.

155 Nougrères (n 18) para 57.
156 Nkonge (n 153) 18, 19.

African Journal on Privacy & Data Protection

To cite: MA Simiyu 'Exploring the legal manoeuvres for an equilibrium between access to information and privacy rights in Kenya and South Africa' (2025) 2
African Journal on Privacy & Data Protection 61-82
https://doi.org/10.29053/ajpdp.v2i1.0004

Exploring the legal manoeuvres for an equilibrium between access to information and privacy rights in Kenya and South Africa

*Marystella A Simiyu**
Africa Senior Legal Advocacy Officer at the International Press Institute

Abstract

An enforcement tension between the right of access to information and privacy is inevitable insofar as the foundation of one right is information disclosure, the other being control of disclosure. Both rights, however, are not absolute in nature and are subject to reasonable and justifiable limitations, allowing the intervention of international, regional and national laws to reconcile competing interests. The balancing of these rights in African legal frameworks is of key interest in Africa where the value of the right to privacy has been contested. However, the evolution of legal instruments such as the African Union Convention on Cyber Security and Personal Data Protection and the African Commission Declaration of Principles on Freedom of Expression and Access to Information in Africa is reflective of the legal adaptation to the contemporary needs of African societies on privacy and information. These instruments together with the Guidelines on Access to Information and Elections in Africa confront the challenges faced with the realisation of both access to information and right to privacy and data

* LLB (Kenyatta University); LLM (Centre for Human Rights, University of Pretoria) & LLD (University of Pretoria) – mssimiyu@gmail.com

protection. This article focuses on the impact of this equilibrium in promoting good governance, transparency and accountability, including during elections, towards nurturing an informed and engaged electorate and public. In dissecting the domestication of the provisions in international and regional instruments, and national approaches to facilitating these rights, the article examines the legal systems in Kenya and South Africa. The article finds that a common anchoring consideration in balancing access to information and privacy rights is a public interest override that outweighs the envisioned harm.

Key words: access to information; privacy; data protection; elections; competing rights

1 Introduction

Paradoxically, the complete enjoyment of human rights rests on limiting the exercise of certain rights that may be in conflict.[1] The rights of access to information and privacy are in a potential collision in as much as they pursue opposing objectives of information disclosure and information control, respectively. However, both rights enjoy fundamental status under international law. The majority of national constitutions reconcile competing interests in rights by imposing limitations. Generally, rights limitations are guided by the principles of legality, legitimate aim, and necessity and proportionality in a democratic society.[2] Absolute rights are only marginally recognised under international law, revealing an expectation of conflicting rights.[3]

The growing corpus of international and national laws has attempted to address the conflict between the right to information and privacy rights. This is especially so in the wake of the implications of globalisation and digital technologies on the exercise of these rights and other rights, including the right to meaningful public and political participation. By employing the human rights approach, this article examines how frameworks at the United Nations (UN) and African levels as well as national legal systems in Kenya and South Africa have approached the reconciliation of these rights. This article is structured in five parts. Part 1 is this introduction. Part 2 unpacks the definition of privacy and its correlation with access to information. Part 3 analyses how the UN and African legal frameworks address the competing interests concerning access to information and privacy. This part zeros in on the substance and implementation of the Guidelines on Access to Information and Elections in Africa using practical examples from

1 A Bilgorajski 'Boundaries and limitations of human rights. A contribution to the discussion' (2023) 27 *Ain Shams Engineering Journal* 68.

2 General Comment 34, Article 19: Freedom of opinion and expression, CCPR/C/GC/34 paras 24-36, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (accessed 5 August 2024).

3 For examples of absolute rights, see art 7 and 8 of the International Covenant on Civil and Political Rights (ICCPR) on freedom from torture and slavery respectively, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (accessed 5 August 2024).

South Africa and Kenya. Part 4 examines how statutes and case law in Kenya and South Africa find the middle ground between privacy and access to information. Part 5 concludes the article.

2 The conceptual intersection between privacy and access to information

Conceptualising privacy has been the subject of considerable intellectual discourse.[4] While there is no accepted consensus on the definition of privacy, the notion of 'access' features strongly in characterisations of the term 'privacy'. Access in this sense is relational and may pertain to access to a person, be it a tangible physical state or intangible psychological state.[5] In one of the early descriptions of privacy, Cooley writes of the right to be left alone.[6] Scholars Warren and Brandeis further depict this right to be left alone or privacy right as a component of a more holistic and evolving portrayal of the right to life and the enjoyment of life.[7] One's desire to exercise control over their state of solitude, anonymity and secrecy, key aspects of privacy, features strongly in this definition.[8] Gerety, similarly, defines privacy as 'an autonomy or control over the intimacies of personal identity'.[9] These definitions place the reigns of regulating the conditions of access to an inner private sanctum on an individual.

The second aspect of access and privacy, on which this article will largely focus, is access to information about a person. The term 'informational privacy' is relevant to this discourse. For example, authors such as Westin define privacy as the 'claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[10] The notion of an individual's control over the conditions surrounding access to information about them has collated the debate and frameworks on privacy as predicated on access to information; in this sense, regulation of what

4 BP Knijnenburg and others 'Introduction and overview' in BP Knijnenburg and others (eds) *Modern socio-technical perspectives on privacy* (2022) 3.

5 I Altman *The environment and social behaviour: Privacy, personal space, territory, and crowding* (1975); R Gavison 'Privacy and the limits of law' (1980) 89 *Yale Law Journal* 423, PJ Wisniewski & X Page 'Privacy theories and frameworks' in BP Knijnenburg and others *Modern socio-technical perspectives on privacy* (2022) 21.

6 T Cooley *A treatise on the law of torts, or the wrongs which arise independent of contract* (1888) 29.

7 SD Warren & LD Brandeis 'The right to privacy' (1890) 4 *Harvard Law Review* 193.

8 Gavison (n 5) 433.

9 T Gerety 'Redefining privacy' (1977) 12 *Harvard Civil Rights-Civil Liberties Law Review* 236. For other definitions of privacy, see H Gross 'The concept of privacy' (1967) 42 *NYU Law Review* 34-36.

10 A Westin *Privacy and freedom* (1967) 7. A similar definition is by BN Ellison and others 'Negotiating privacy concerns and social capital needs in a social media environments' in S Trepte & L Reinecke (eds) *Privacy online* (2011) 19-21 who define privacy as 'the ability of individuals to control when, to what extent, and how information about the self is communicated to others'. Also see J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 19.

is retained and what is disclosed from the private to the public realm.[11] This definition in itself acknowledges that information about a person may not be in their sole possession or control, but others may have access to one's information. Consequently, a collective responsibility is imposed on others to protect another's right to privacy and unconsented and unreasonable access to their information.[12]

Often, 'privacy' and 'data protection' are used concomitantly and even sometimes synonymously, though discourse on their similarity or identicalness has been contentious.[13] As definitional purists argue, data protection specifically relates to safeguards emanating from the modalities of processing personal data (information of 'an identified or identifiable natural person'), which may cross the confines of the private sphere that the right to privacy protects.[14] Norms on data protection canvas how information is collected, stored, used and disseminated which has a correlation with the right to privacy but may exceed its formulation in its application.[15] Makulilo concluded that 'privacy and data protection are two distinct and separate concepts although they have overlapping objectives. The differences between the two concepts reside in their scope, goals, and content.'[16] Notably, some authors have adopted the terms 'data' and 'information privacy' to temper the tension between data protection and privacy conceptualisation.[17] Coalescing concurring and differing debates on privacy and data protection, a common ground that largely unifies the different discourses, is the presence of information and the exercise of control on its disclosure and management. This article underscores the conditions for information disclosure that conform to or conflict with the right to privacy. The ensuing context is characterised by globalisation and revolutionary technological advancements that have opened up frontiers for facilitating access to information and simultaneously complicated the ability of individuals to control information retention and disclosure. The intervention and adaptation of the law to this reality become crucial to protect personal and informational privacy and access to information.

11 Wisniewski & Page (n 5) 16-17, X Heng and others *Examining the formation of individual's privacy concerns: Toward an integrative view* (2008).

12 H Jia & H Xu 'Measuring individuals' concerns over collective privacy on social networking sites (2016) 10 *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 1-2.

13 AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) *International Data Privacy Law* 164-165.

14 C Cuijpers 'A private law approach to privacy: Mandatory law obliged?' (2007) 4 *Scripted* 312. Art 4 of the General Data Protection Regulation (GDPR) defines personal data as 'any information relating to an identified or identifiable natural person ("data subject")'.

15 P de Hert & S Gutwirth 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalism in action' in S Gutwirth and others (eds) *Reinventing data protection?* (2009) 3-10.

16 Makulilo (n 13) 166.

17 PM Schwartz & JR Reidenberg *Data privacy law: A study of United States data protection* (1996) 5; SK Karanja 'Schengen information system and border control co-operation: A transparency and proportionality evaluation' PhD thesis, University of Oslo, 2006 86; LA Bygrave 'Privacy protection in a global context – A comparative overview' (2004) 47 *Scandinavian Studies in Law* 321-322.

3 Reconciling competing interests of privacy and access to information in the United Nations and African legal frameworks

The legal status of the right to privacy evolved from discourse to common law protection to prescriptive with legal recognition and protection in key human rights frameworks such as article 12 of the Universal Declaration of Human Rights (Universal Declaration);[18] article 17 of the International Covenant on Civil and Political Rights (ICCPR); and a majority of national constitutions including on the African continent. Article 17 of ICCPR prohibits 'arbitrary or unlawful interference with' a person's 'privacy, family, home or correspondence', or unlawful attacks on their honour and reputation. The exclusion of privacy rights in the African Charter on Human and Peoples' Rights (African Charter)[19] has inspired discussion on the place of privacy in Africa. Some authors have argued that the omission of the right to privacy in the African Charter should not lead to the conclusion that an individual's right to privacy lacks value in African societies.[20] This argument is often grounded in Africa's collectivist culture.[21] The articulation of the right to privacy in current African legal frameworks challenges arguments on its utility in contemporary African society. Case in point, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), which took effect in June 2023, is a homegrown instrument that outlines state obligations with regard to personal data protection.[22] Admittedly, the development of the instrument was inspired by European legal frameworks such as the European Union Data Protection Directive 95/46/EC;[23] the Council of Europe Convention 108;[24] and the Organisation for Economic Co-operation

18 Universal Declaration of Human Rights, https://www.ohchr.org/en/human-rights/universal-declaration/translations/english (accessed 10 August 2024).

19 African Charter on Human and Peoples' Rights, https://au.int/sites/default/files/treaties/36390-treaty-0011_-_african_charter_on_human_and_peoples_rights_e.pdf (accessed 5 August 2024).

20 In P Boshe 'A quest for an African concept of privacy'. Iin LA Abdulrauf & H Dube (eds) *Data privacy law in Africa: Emerging perspectives* (2024) 24-26 the author debunks the myth of African privacy as foreign to traditional African societies. Also see AB Makulilo 'Data privacy in Africa: Taking stock of its development after two decades' in LA Abdulrauf & H Dube (eds) *Data privacy law in Africa: Emerging perspectives* (2024) 61 where Makulilo critics Bygrave and Gutwirth for misinterpreting the absence of a right to privacy provision in the African Charter to mean a devaluation of the individual right to privacy over community interests in S Gutwirth *Privacy and the information age* (2002) 24 and Bygrave (n 17) 328.

21 As above.

22 Malabo Convention, https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 5 August 2024). Also see Lawyers Hub 'Africa privacy report 2023/2024: A review of policy trends and digital frontiers in Africa's data protection landscape' (2023), https://www.ictworks.org/wp-content/uploads/2024/05/Africa-Privacy-Report.pdf (accessed 5 August 2024).

23 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046 (accessed 5 August 2024).

24 https://www.coe.int/en/web/data-protection/convention108-and-protocol (accessed 5 August 2024).

and Development (OECD) Privacy Guidelines.[25] All the same, the Malabo Convention addresses privacy and data protection issues in the African context.

Other binding and non-binding instruments have articulated the right to privacy in Africa, such as article 10 of the African Charter on the Rights and Welfare of the Child (African Children's Charter), which protects the right to privacy of children.[26] The African Children's Charter, however, was inspired by the UN Convention on the Rights of the Child (CRC), which contains a similar provision.[27] Additionally, principle 40 of the Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019 Declaration) articulates everyone's right to privacy and the protection of their personal information.[28]

Shifting gears to the right to information, its original formulation under international law is under freedom of expression encompassing freedom of expression, right to information, and media freedom. At the UN level, the right to information originates from the freedom of expression definition as the 'freedom to seek, receive and impart information and ideas'.[29] Under article 9 of the African Charter, it is simply 'the right to receive information'. Soft law instruments have significantly elaborated the substance of the umbrella of rights encapsulating free expression to peel back the essence of the right to information. General Comment 34 on article 19 of ICCPR, for instance, defines it as the right to access information including records possessed by public bodies or other entities that conduct public functions.[30] General Comment 34 proceeds to obligate states to ensure proactive disclosure of information of public interest and the passage of the necessary legal frameworks to enforce the right to information.[31] Under General Comment 34, one can exercise the right against the state and public bodies. However, successive frameworks have narrowly expanded the scope of duty bearers.

25 For the OECD Privacy Guidelines, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188 (accessed 5 August 2024). Also see Makulilo (n 20) 63-64; LA Abdulrauf & CM Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67-97.

26 https://au.int/sites/default/files/treaties/36804-treaty-african_charter_on_rights_welfare_of_the_child.pdf (accessed 6 August 2024).

27 Preamble to the African Children's Charter and art 16 of CRC, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child (accessed 6 August 2024). Also see A Lloyd 'A theoretical analysis of the reality of children's rights in Africa: An introduction to the African Charter on the Rights and Welfare of the Child' (2002) 2 *African Human Rights Law Jour*nal 16-17.

28 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/ati/Declaration_of_Principles_on_Freedom_of_Expression_ENG_2019.pdf (accessed 6 August 2024). The African Commission on Human and Peoples' Rights first adopted the instrument in 2002. The current 2019 version is a revision of the original Declaration and incorporates stronger protection for freedom of expression and access to information in light of digital advancement.

29 Art 19 ICCPR; art 19 Universal Declaration.

30 General Comment 34 para 18, https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf (accessed 6 August 2024).

31 General Comment 34 para 19.

The right to information under the African Charter is augmented by binding and non-binding instruments that provide context-specific obligations to facilitate access to information. The interdependent character of rights is revealed in the formulation of these provisions with access to information seen as an enabling right to other fundamental rights. For example, article 2 of the African Charter on Democracy, Elections and Governance (African Democracy Charter) links access to information to improved 'democracy, elections and governance';[32] article 4 of the African Union Convention on Preventing and Combating Corruption includes access to information as a measure towards addressing corruption and related offences;[33] and article 6 of the African Charter on Values and Principles of Public Service and Administration requires the realisation of the right to information in public service and administration towards effective public service delivery.[34] An underlying thrust of these instruments is to course-correct and counter the endemic culture of secrecy, maladministration, corruption and impunity in African governments, and enhance transparency, accountability and meaningful public participation.[35] The dichotomy between the ensuing secrecy culture in public institutions and contentious secrecy legislation in some African countries against the growing corpus of freedom of information laws in Africa unveils a tension not only within human rights but also within the state and institutional culture.[36] Relatedly, Fitzpatrick argues that the 'tendency of governing elites to confuse "the life of the nation" with "the survival of the regime" creates a grave risk that derogations and limitations on expression and information rights will be excessive'.[37]

Cognisant of the implication of state secrecy on access to information, the international mechanisms of the UN Special Rapporteur on Freedom of Opinion and Expression, the Organisation for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media, and the Organisation of American States (OAS) Special Rapporteur on Freedom of Expression adopted

32 Art 2 African Democracy Charter, https://au.int/sites/default/files/treaties/36384-treaty-african-charter-on-democracy-and-governance.pdf (accessed 6 August 2024).

33 Art 4 African Union Convention on Preventing and Combating Corruption, https://anticorruption.au.int/sites/default/files/files/2021-06/combattingcorruptionconvention a5v2enreduced.pdf (accessed 6 August 2024).

34 Art 6 African Charter on Values and Principles of Public Service and Administration, https://au.int/sites/default/files/treaties/36386-treaty-charter_on_the_principles_of_public_service_and_administration.pdf (accessed 6 August 2024).

35 See the Preambles to the instruments in addition to the specific sections.

36 On secrecy laws, see AO Salau 'The right of access to information and national security in the African regional human rights system' (2017) 17 *African Human Rights Law Journal* 378; OA Osawe 'A comparative analysis of the right of access to information under the Nigerian Freedom of Information Act 2011 and the South African Promotion of Access to Information Act 2001' (2022) 22 *African Human Rights Law Journal* 476-492; J Klaaren 'The South African "Secrecy Act": Democracy put to the test' in H Botha, N Schaks & D Steiger (eds) *The end of the representative state? Democracy at the Crossroads – A German-South African perspective* (2016) 131-156.

37 J Fitzpatrick 'Introduction' in S Coliver & P Hoffman (eds) *Secrecy and liberty: National security, freedom of expression and access to information* (1999) xi.

the Joint Declaration on Access to Information and Secrecy Legislation in 2004. The Declaration provides:[38]

> The right of access should be subject to a narrow, carefully tailored system of exceptions to protect overriding public and private interests, including privacy. Exceptions should apply only where there is a risk of substantial harm to the protected interest and where that harm is greater than the overall public interest in having access to the information. The burden should be on the public authority seeking to deny access to show that the information falls within the scope of the system of exceptions.

The right to information under the African Charter is further refined by a tripartite soft law structure found in the 2019 Declaration, the Model Law on Access to Information for Africa (2013 Model Law),[39] and the Guidelines on Access to Information and Elections in Africa (2017 Guidelines).[40] The 2013 Model Law provides that its objective is to give effect to operationalise this right as guaranteed by the African Charter to 'any information held by a public body or relevant private body; and any information held by a private body that may assist in the exercise or protection of any right'. Crafted in similar terms, the 2019 Declaration and the 2017 Guidelines combined with the 2013 Model Law indeed form the corpus of frameworks that expand the scope of actors upon whom the right of access to information is enforceable.

First, public bodies and relevant private bodies have a duty to proactively disclose information.[41] The proactive disclosure of information principle anticipates that information disclosures are not predicated on a request but are rather done routinely in the course of duty.[42] Privacy considerations come into play given some of the information held by these bodies may be confidential information or personal data subject to legal protection. Persons can exercise their right of access to information, including access to one's personal data, against three duty bearers:[43]

- a public body characterised as an entity established by the Constitution or other law, or is part of government;
- 'a relevant private body', meaning an otherwise private body that is owned totally or partially or directly or indirectly 'controlled or financed by public funds', or undertakes 'a statutory or public function or' service; and

38 Joint Declaration on Access to Information and Secrecy Legislation, https://www.article19.org/resources/joint-declaration-access-information-secrecy-legislation/ (accessed 6 August 2024).
39 2013 Model Law, https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/model_law_on_ati_in_africa/model_law_on_access_to_infomation_en.pdf (accessed 6 August 2024).
40 https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/guidelines_on_access_to_information_and_elections_in_africa_en.pdf (accessed 7 August 2024). The Guidelines were adopted by the African Commission in 2017.
41 Sec 7 2013 Model Law.
42 Part 1 2017 Guidelines.
43 Part 1 sec 1 2013 Model Law.

- a private body but the enforceability of access is conditional upon the exercise or protection of another right.

The presence of a legal framework on privacy and data protection that is concisely drafted, accessible and enforced by competent and independent authorities dovetails with the right to information. There is a reasonable expectation to know to what extent governments can curtail an individual's right to privacy in the name of the right to information as well as the safeguards implemented to prevent arbitrary and unlawful infringement of the right to privacy. General Comment 16 on the right to privacy emphasises the need for information on authorities allowed to interfere with their right to privacy, the manner and extent of the interference and recourse and remedy in the event of a violation.[44]

While the Malabo Convention's objective on personal data commits African states to develop laws to strengthen human rights, especially the protection of physical data and privacy, it attaches a caveat that these measures should not prejudice the free flow of data.[45] The Malabo Convention and the 2019 Declaration stipulate the guiding principles for the legal processing of personal data, including 'consent and legitimacy, legality and fairness, purpose, adequacy and relevance, accuracy, transparency, and confidentiality and security'.[46] These principles further demarcate the boundaries of privacy and information access and disclosure. Access to information is also emphasised with regard to the processing of personal information. Among the rights of a data subject in the Malabo Convention and the 2019 Declaration is the right to information on the type, scope, purpose, recipients, and timelines with regard to the information processed about them. The data subject also has the right to access this information and may object to the processing of the data or rectify or erase the information.[47] Data subjects, therefore, can submit an access to information request to a data controller or processor for their own personal data to manage access to their information.

Also, an examination of the 2019 Declaration shows that from the outset it recognises the correlation between free expression (including the right to information) and privacy towards enabling the right to dignity.[48] The 2019 Declaration guarantees the right to privacy both offline and online and the protection of personal information under principle 40. The Declaration further outlines state obligations in adopting privacy and data protection laws that comply with international laws and standards.[49] The balancing and trade-off between privacy, data protection and information disclosure beyond one's private

44 UN Human Rights Committee CCPR General Comment 16: Article 17 (Right to privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation para 6, https://www.refworld.org/legal/general/hrc/1988/en/27539 (accessed 7 August 2024).
45 Art 8 Malabo Convention.
46 Art 13 Malabo Convention; art 42(2) 2019 Declaration.
47 Art 16 Malabo Convention; Principle 42(3) 2019 Declaration.
48 Preamble to 2019 Declaration.
49 Principle 42 2019 Declaration.

sphere is seen in various provisions. Towards protecting data or information privacy, the Declaration imposes both negative and positive state obligations. The prohibition against 'indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications' and targeted surveillance that contradicts international laws and standards is a negative obligation aimed at ensuring the state respects the right to privacy.[50] The state's positive obligation emanates from the duty to adopt laws for 'the protection of personal information, privacy and communication surveillance of individuals in accordance with international human rights law and standards' as well as other safeguards.[51]

As of August 2024, at least 36 countries in Africa have passed data protection laws.[52] Fewer countries have adopted access to information laws at about 28 African states.[53] Cabo Verde, which was the trendsetter in Africa in adopting data protection laws in 2001, only adopted its access to information law in 2022. Some authors have credited the Brussels Effect as the impetus behind the uptake of domestic data privacy laws in Africa.[54] Specifically, 'the adequacy requirement' under articles 25 to 26 of the now-repealed Data Protection Directive 95/46/EC predicates data transfer to third-party countries on an 'adequate level' of protection.[55] Similarly, the earlier-mentioned influence of the European data protection regime on the substance of the Malabo Convention and many national data protection laws has drawn concern about the absence of an African-centred methodology for regulating privacy and data protection in African countries.[56] Reflecting that privacy provisions in African constitutions were similarly inspired by the constitutions of imperial governments, it rests on enforcement actors, including the judiciary, to ensure that the interpretation of national statutory provisions is reflective of the African context while protecting fundamental rights such as access to information. This is especially crucial because of concerns over poor implementation of laws despite a demand for public interest information

50 Principle 41 2019 Declaration.
51 Principles 41(2), (3) & 42 2019 Declaration.
52 These are Algeria (2018), Angola (2011), Benin (2009), Botswana (2018), Burkina Faso (2004), Cabo Verde (2001), Chad (2015), Côte d'Ivoire (2013), Egypt (2020), Equatorial Guinea (2016), Eswatini (2022), Gabon (2011), Ghana (2012), Guinea (2016), Kenya (2019), Lesotho (2011), Madagascar (2014), Mali (2013), Mauritania (2017), Mauritius (2017), Morocco (2009), Niger (2017), Nigeria (2023), Republic of Congo (2019), Rwanda (2021), São Tomé & Príncipe (2016), Senegal (2008), Seychelles (2003), Somalia (2023), South Africa (2013), Tanzania (2022), Togo (2019), Tunisia (2004), Uganda (2019), Zambia (2021), Zimbabwe (2021). Ethiopia, Malawi and Namibia have draft laws. ALT Advisory 'Which African countries have a data protection law?',https://dataprotection.africa/which-african-countries-have-a-data-protection-law/ (accessed 8 August 2024).
53 These are Angola, Benin, Burkina Faso, Cabo Verde, Côte d'Ivoire, Ethiopia, Ghana, Guinea, Kenya, Liberia, Malawi, Morocco, Mozambique, Namibia, Niger, Nigeria, Rwanda, Seychelles, Sierra Leone, South Africa, South Sudan, Sudan, Tanzania, Togo, The Gambia, Tunisia, Uganda, Zambia and Zimbabwe. AFIC 'Access to information laws in Africa', https://www.africafoicentre.org/foi-laws/?cp=3 (accessed 8 August 2024).
54 Boshe (n 20) 23; Makulilo (n 20) 69-71; Makulilo (n 13) 42-50.
55 As above.
56 G Greenleaf & B Cottier 'Comparing African data privacy laws: International, African and regional commitments' University of New South Wales Law Research Series (2020) 33; Boshe (n 20) 30-34.

and privacy and data protection in Africa.[57] In subsequent parts, this article analyses how courts in Kenya and South Africa have confronted this conundrum.

3.1 The contribution of the African Commission 2017 Guidelines to the information versus privacy debate and its implementation in South Africa and Kenya

The Guidelines on Access to Information and Elections were adopted by the African Commission on Human and Peoples' Rights (African Commission) in 2017 to reinforce the protection of the right to freedom of expression and access to information particularly during elections.[58] The 2017 Guidelines underscore 'the principle of proactive disclosure of information' throughout the election period as a conduit for enhanced accountability of electoral stakeholders and promoting credibility, integrity and stability during African elections.[59] The interdependence between access to timely, credible, relevant and accurate information with meaningful political participation is an underlying thrust of the 2017 Guidelines. Meaningful political participation, including exercising the right to vote, envisages the active participation of an informed electorate in the elections and other democratic processes who can freely exercise their right to expression, association and assembly.[60]

The realisation of access to information during elections transforms voting from a passive exercise to an engaging experience by informed voters. That being said, various historical, social, cultural, political and economic considerations and biases influence voter choice in many African elections that are not anchored on issues. Blind affiliation to group interests driven by ethnicity, tribe and religion, among others, or personality politics without a corresponding reflection on issues and track record are an Achilles heel of meaningful participation in elections in Africa.[61] Arguably, through concerted civic and voter education and access to

57 A Okello, S Sunderland & J Asunka 'Veiled transparency: Access to public information remains elusive despite progress on right-to-information laws' (22 February 2024) 771 *Afrobarometer* 3, https://www.afrobarometer.org/wp-content/uploads/2024/02/AD771-PAP10-Access-to-public-information-remains-elusive-across-Africa-Afrobarometer-20feb24.pdf (accessed 9 August 2024); CIPESA 'Mapping and analysis of privacy laws in Africa' (2021), https://cipesa.org/wp-content/files/briefs/Mapping_and_Analysis_of_Privacy_Laws_in_Africa_2021.pdf (accessed 9 August 2024).

58 Rationale and objectives of the Guidelines.

59 As above.

60 UN Human Rights Committee General Comment No 25: The right to participate in public affairs, voting rights and the right of equal access to public service (art 25) paras 8, 9 & 12, https://www.equalrightstrust.org/ertdocumentbank/general%20comment%2025.pdf (accessed 9 August 2024). Also see *President of the Republic of South Africa & Others v M & G Media Ltd* CCT 03/11 [2011] ZACC 32; 2012 (2) BCLR 181 (CC); 2012 (2) SA 50 (CC) (29 November 2011), https://www.saflii.org/za/cases/ZACC/2011/32.html (accessed 9 August 2024); *My Vote Counts NPC v Minister of Justice and Correctional Services & Another* CCT249/17 [2018] ZACC 17; 2018 (8) BCLR 893 (CC); 2018 (5) SA 380 (CC) (21 June 2018) (*MVC 2018*) para 34, https://www.saflii.org/za/cases/ZACC/2018/17.html#_ftn29 (accessed 9 August 2024).

61 JT Andrews & K Inman 'Explaining vote choice in Africa's emerging democracies' (2009) Conference Paper - 2009 meeting of the Midwest Political Science Association, https://fsi-

information, fledgling African democracies can course-correct and nurture a culture of issue and performance-based voter choice.

Uniquely, the 2017 Guidelines identify eight key electoral stakeholders and outline the information which, at the minimum, they should disclose to the electorate and public during elections. The electoral stakeholders are 'appointing authorities of election management bodies (EMBs), EMBs, political parties and candidates, civil society organisations (CSOs), law enforcement agencies, media regulatory bodies, media and online media platform providers, and election observers and monitors'.

Since 2019, the Centre for Human Rights, University of Pretoria (CHR) has undertaken a country assessment of domestic compliance with the Guidelines that covered South Africa (2019),[62] Uganda (2020),[63] The Gambia (2021)[64] and Kenya (2022).[65] While there are varying levels of compliance in the different countries influenced by democratic culture, legislative coherence, institutional strength, and resource capacity, among others, the reports reveal an overall need to enhance knowledge of the Guidelines and promote its mainstreaming in the activities of electoral stakeholders.[66] Guidelines 31 to 34 strive to promote the implementation of the 2017 Guidelines by mandating state adoption of 'legislative, administrative, judicial and other measures' to implement the soft law. States are also required to disseminate the Guidelines to relevant electoral stakeholders and ensure effective training. Compliance measures should be captured in the periodic country reports 'submitted to the African Commission under article 62 of the African Charter'.

Relevant to privacy, data protection and access to information, the CHR reports, as well as advocacy actions on the implementation of the proffered recommendations, reveal instances of conflict between access to information and privacy and data protection obligations. A review of the Guidelines reveals a singular focus on information disclosure. The Guidelines are structured to outline the categories of information electoral stakeholders should disclose

live.s3.us-west-1.amazonaws.com/s3fs-public/evnts/media/Andrews_Inman_Explaining_Vote_Choice_in_African_Democracies.pdf (accessed 11 August 2024).

62 CHR and others 'Proactive disclosure of information and elections in South Africa' (2020), https://www.chr.up.ac.za/images/researchunits/dgdr/documents/reports/Proactive_Disclosure_of_Information_and_Elections_in_South_Africa.pdf (accessed 11 August 2024).

63 PD Mutesasira & DR Ruhweza 'Proactive disclosure of information and elections in Uganda' (2023), https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Proactiive_Disclosure_of_Information_During_Elections_Uganda.pdf (accessed 11 August 2024).

64 J Grey-Johnson 'Proactive disclosure of information and elections in The Gambia' (2023), https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Proactiive_Disclosure_of_Information_During_Elections_Gambia.pdf (accessed 11 August 2024).

65 L Mute 'Proactive disclosure of information and elections in Kenya' (2023), https://www.chr.up.ac.za/images/researchunits/dgdr/documents/resources/Proactiive_Disclosure_of_Information_During_Elections_Kenya.pdf (accessed 11 August 2024).

66 Insights from electoral stakeholder engagements organised by the CHR in which the author of this article facilitated as a project lead.

during the elections. Not surprisingly, EMBs bear the most burden in information disclosure on both internal records as well as other election records, given their election administration mandate.[67] The potential dilemma of conflicting proactive disclosure obligations with privacy and data protection does not receive a mention in the Guidelines. This is not to say that the Guidelines did not contemplate the notion of competing rights. For example, the stipulation for responsible authorities to refrain from implementing internet shutdowns further provides that in exceptional cases necessitating an internet shutdown, the reasons shall be proactively disclosed and the limitation complies with the three requirements of lawfulness, legitimate aim and necessity and proportionality in addition to prior judicial review.[68] Interestingly, among the stakeholders, the Guidelines only indicate a general caveat on proactive disclosure duties of CSOs and this is based on exceptional cases where it is evident that their operations may suffer demonstrable harm.[69]

Political parties are also data controllers and data processors during elections. The 2017 Guidelines perceive political parties through the lens of a duty bearer to disclose information with no mention of their privacy and data protection obligations. Guideline 21 requires states to enact the relevant laws including on the proactive disclosure by political parties of received public and private funding, campaign expenditures, and annual audited financial reports. The orientation of political parties has traditionally been categorised under private bodies but their status as private bodies blurs when some elements of a public body breach this boundary such as through the receipt of public funds.[70] In South Africa, courts have affirmed the position of political parties as voluntary associations and private bodies.[71] However, in their capacity as private bodies, they have information disclosure obligations including on private funding, that the Constitutional Court of South Africa linked to the electorate's ability to meaningfully exercise their right to vote and make informed decisions.[72] This obligation also extends to independent candidates. In the fulfilment of this obligation, political parties and candidates may disclose personal data about private funders which, in some cases, may lead to prejudices emanating from supporting certain parties or candidates. In South Africa, the decision of the Constitutional Court led to the amendment of the Promotion of Access to Information Act (PAIA),[73] and the adoption of the

67 Guidelines 13-19 2017 Guidelines.
68 Guidelines 26-28 2017 Guidelines.
69 Guideline 30 2017 Guidelines.
70 I Biezen 'Political parties as public utilities' (2004) 10 *SAGE* 7021-702; A Gauja 'Political parties: Private associations or public utilities?' in J Gardner (ed) *Comparative election law* (2022) 177-192.
71 *Institute for Democracy in South Africa & Others v African National Congress & Others* (9828/03) [2005] ZAWCHC 30; 2005 (5) SA 39 (C); [2005] 3 All SA 45 (C); 2005 (10) BCLR 995 (C) (20 April 2005) *(IDASA v ANC)*, https://www.saflii.org/za/cases/ZAWCHC/2005/30.html (accessed 11 August 2024).
72 MVC 2018 (n 60) paras 33 & 48. The MVC decision overturned the decision in *IDASA v ANC* (n 71) that exempted political parties from disclosing private funding by nature of their private body status.
73 PAIA Amendment Act 31 of 2019, https://www.gov.za/sites/default/files/gcis_document/202007/43388gon630.pdf (accessed 11 August 2024).

Political Party Funding Act (PPFA) in 2018 which fulfils Guideline 21. In Kenya, section 16 of the Election Campaign Financing Act, 2013[74] regulates disclosure of funding by political parties. However, the Act's implementation has suffered in the wake of its suspension from coming into force until the 2017 elections and lack of political will.[75]

Instances in the Guidelines that necessitate privacy considerations include on disclosure of the voter register. Guideline 17 obligates EMBs to proactively disclose the voter's register with voter's identification information including their full name, identity card number, picture (if available), age and gender. Data protection considerations require EMBs and other data controllers and processors to consider data protection principles, particularly purpose limitation and data minimisation before disclosing such personal details in the full register. Therefore, it is important to read these provisions together with international privacy and data protection standards, and relevant national laws and case law.

National legislation is important to balance privacy and access to information during elections. In Kenya, the Independent Electoral and Boundaries Commission (IEBC) is obligated to apply the data protection principles as outlined in the Data Protection Act in processing the personal data of voters.[76] The voter's roll contains biometric data as well as other personal information including their name, identity number, sex, postal and residential address, and phone and email contact details.[77] South Africa's voter's register contains the identity number, consecutive number, voter's name and voter's address or ordinary residence but no mention of a photograph.[78] A participating political party can request a copy of the voter's roll without charge but will be subject to a fee if they want the version with additional information on the addresses of voters.[79] They are also tasked to only use the information for election purposes, failing which they are guilty of an offence.[80] This makes political parties data controllers and processors with responsibilities to protect the privacy and data of voters.

74 42 of 2013, https://www.iebc.or.ke/uploads/resources/SrIlWeBWMH.pdf (accessed 11 August 2024).

75 G Ndirangu 'No limits: Campaign spending spikes ahead of Kenyan elections' *Al Jazeera* 22 June 2022, https://www.aljazeera.com/features/2022/6/22/no-limits-campaign-spending-spikes-ahead-of-kenyan-elections (accessed 12 August 2024); Mzalendo 'Campaign financing legislation and the 2022 general elections', https://mzalendo.com/posts/campaign-financing-legislation-and-the-2022-genera/ (accessed 12 August 2024). See also Election Campaign Financing (Amendment) Bill, 2020, https://www.iebc.or.ke/uploads/resources/iGNrE6ZL95.pdf (accessed 12 August 2024).

76 Sec 25(i) IEBC Act 9 of 2011, https://www.iebc.or.ke/uploads/resources/8Z5fmROhVD.pdf (accessed 8 August 2024).

77 Sec 8 The Elections (Registration of Voters) Regulations, http://kenyalaw.org:8181/exist/kenyalex/sublegview.xql?subleg=CAP.%207#doc-0 (accessed 8 August 2024).

78 Regulation 10 Voter Registration Regulations 1998 as amended, https://www.gov.za/sites/default/files/gcis_document/202402/50066gon4307.pdf (accessed 12 August 2024).

79 Regulation 8 Voter Registration Regulations, 1998 as amended.

80 Sec 16(4) Electoral Act as amended, https://www.gov.za/documents/electoral-act (accessed 12 August 2024).

Privacy and data protection responsibilities of political parties are heightened in the information age. Digital technologies have refined data-driven political campaigning and strategising that has raised concerns around the data of voters and the wider public.[81] A breach into the private sphere is evident in the growing trend of unsolicited and targeted political messaging during elections sent through personal devices or social media platforms.[82] Increasing integration of technology in election administration in Africa coupled with empirical evidence of data breaches of voter information, as in the case of Kenya in the 2022 elections,[83] or closed political party lists information, as was the case in South Africa during the 2024 elections[84] reveal a need for electoral stakeholders to reinforce data privacy practices in compliance with existing legislation. Information Regulators and Data Protection Authorities have adopted regulations to address the tensions of access to information and privacy. The Office of the Data Protection Commissioner (ODPC) in Kenya published the Guidance Note on the Processing of Personal Data for Electoral Purposes during the 2022 election period, aimed at guiding data processors, including political parties and candidates.[85] In 2019, the South Africa Information Regulator published a Guidance Note on the Processing of Personal Information of a Voter by a Political Party in Terms of the Protection of Personal Information Act, 4 of 2013.[86] However, there is a need for better compliance and wider civic education on information and privacy rights.[87]

81 CJ Bennett & D Lyon 'Data-driven elections' (2019) 8 *Internet Policy Review* 3-4.

82 Privacy International 'Challenging data exploitation in political campaigning' (2020) 5-6, https://privacyinternational.org/sites/default/files/2020-06/PI%20Recs_Challenging%20Data%20Exploitation%20in%20Political%20Campaigning.pdf (accessed 12 August 2024).

83 J Otieno 'Kenyans protest registration as party members without consent' *The Star* 19 June 2021, https://www.the-star.co.ke/news/2021-06-19-kenyans-protest-registration-as-party-members-without-consent/ (accessed 12 August 2024). Also see R Mosero 'In Kenya's 2022 elections, technology and data protection must go hand in hand' Carnegie Endowment for International Peace (8 August 2022), https://carnegieendowment.org/2022/08/08/in-kenyas-2022-elections-technology-and-data-protection-must-go-hand-in-hand-pub-87647 (accessed 12 August 2024).

84 A Moyo 'IEC fires official for leaking political candidate lists' *IT Web* 12 March 2024, https://www.itweb.co.za/article/iec-fires-official-for-leaking-political-candidate-lists/xnklOqz1AKjM4Ymz (accessed 12 August 2024).

85 Mosero (n 83). The original Guidance Note was no longer available on the ODPC's website at the time of writing this article.

86 https://inforegulator.org.za/wp-content/uploads/2020/07/InfoRegSA-GuidanceNote-PPI-PolParties-1.pdf (accessed 13 August 2024).

87 IR 'Information Regulator shares outcomes of complaints investigated and assessments conducted in relation to PAIA and POPIA' (26 March 2024), https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-BRIEFING-STATEMENT-OF-THE-INFORMATION-REGULATOR-ON-OUTCOMES-ON-COMPLAINTS-ASSESSMENTS.pdf (accessed 13 August 2024). Also see MA Bouke and others 'African Union Convention on Cyber Security and Personal Data Protection: Challenges and future directions' (2023) *arXiv* 6, https://arxiv.org/pdf/2307.01966 (accessed 13 August 2024).

4 The interplay of privacy, data protection and access to information in the broader legal framework in South Africa and Kenya

Both South Africa and Kenya have adopted access to information and data protection laws and set up the required enforcement agencies. Arguably, South Africa is more advanced in anchoring these laws through supporting policies, institutions and case law though the effectiveness of implementation has been contentious.[88] South Africa heralded the adoption of information laws in Africa with the enactment of PAIA in 2000.[89] The Act was operationalised in 2001. PAIA is the statute envisioned under article 32(2) of the Constitution to enable access to information in the possession of the 'state, or another person' and that is necessary for 'the exercise or protection of any rights'.[90] The status of the legislation in relation to article 32 has been interpreted in the courts of law with PAIA affirmed as the vehicle for facilitating the constitutional right of access to information.[91] Further access to information is endorsed as a means towards reinforced 'human rights culture, social justice, transparency, accountability and effective governance of all public and private bodies'.[92] From the outset, the absolute character of access to information is negated with PAIA subjecting the exercise of the right to justifiable limitations including 'the reasonable protection of privacy, commercial confidentiality, and effective, efficient and good governance' and such as to balance access to information with any other rights.[93] Relevant to the crux of this article, the below focuses on the extent privacy rights may warrant the restriction of access to information.

Assessing the bounds of information disclosure within the confines of the law requires enforcement agencies to consider access to information frameworks alongside privacy and data protection laws; relevant to South Africa, PAIA and the Protection of Personal Information Act (POPIA). This is crucial to safeguard against unreasonable information disclosure as articulated under section 34 of PAIA.[94] In an effort to reconcile the interests of access to information and privacy rights, PAIA outlines either mandatory or discretional obligations in disclosing

88 DL Marais, M Quayle & JK Burns 'The role of access to information and public participation in governance: A case study of access to policy consultation records in South Africa' (2017) 9 *African Journal of Public Affairs* 36-49; MG Mojapelo 'A framework towards the implementation of freedom of information legislation in South Africa' (2024) *Emerald Insight*, https://www.emerald.com/insight/content/doi/10.1108/IDD-11-2022-0121/full/pdf?title=a-framework-towards-the-implementation-of-freedom-of-information-legislation-in-south-africa (accessed 13 August 2024).

89 PAIA https://www.gov.za/sites/default/files/gcis_document/201409/a2-000.pdf (accessed 13 August 2024).

90 Art 9(A) PAIA.

91 *IDASA v ANC* (n 71); *Kerkhoff v Minister of Justice and Constitutional Development & Others* 2011 (2) SACR 109 (GNP) [2010] ZAGPPHC 5; 14920/2009 (10 February 2010), https://www.saflii.org/za/cases/ZAGPPHC/2010/5.html (accessed 13 August 2024).

92 Secs 9(c) & (e) PAIA.

93 Sec 9(b) PAIA.

94 Also see the judgment in *Smuts NO & Others v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism & Others*

certain information that is protected from disclosure on privacy grounds. For both public and private bodies, considerations include 'unreasonable disclosure of third party information of a natural person including a deceased person';[95] third party commercial information such as trade secrets or own commercial information in the case of a private body;[96] breach of confidentiality or disclosure that may threaten the receipt of future confidential information for a public body;[97] protection of the safety of persons or property;[98] unwaived legal privilege considerations;[99] and protection of research data of a third party, or research data of the public or private body.[100]

Other privacy considerations and exemptions from disclosure for a public body on privacy grounds include some records of the South African Revenue Service (SARS) unless requested by the tax subject or their representative;[101] police records 'in bail proceedings, and law enforcement and legal proceedings';[102] reasonable threats to the national defence, security and international relations;[103] material threats to national economic interests and financial welfare and the public body's commercial activities;[104] impediments to the formulation or success a policy, or public decision making;[105] and 'manifestly frivolous or vexatious requests' or requests that may considerably and unreasonably redirect resources.[106]

While PAIA stipulates specific exemptions to these considerations, it also provides a general public interest override with regard to grounds of refusal based on privacy except concerning SARS records under section 35 of PAIA.[107] In particular, the public interest override operates if information disclosure reveals a substantial legal offence or violation; or 'imminent and serious public safety or environmental risk'.[108] Further, the enforcement agency must weigh whether the public interest in the information disclosure supersedes the contemplated harm.

Kenya's Access to Information Act (ATI), on the other hand, is a fairly recent enactment having come into force in 2016.[109] The equally important

(1199/2021) [2022] ZAECMKHC 42 (26 July 2022) paras 41-43, https://www.saflii.org/za/cases/ZAECMKHC/2022/42.html (accessed 13 August 2024).

95 Secs 34 & 63 PAIA.
96 Secs 36, 64 & 68 PAIA.
97 Secs 37 & 65 PAIA.
98 Secs 38 & 66 PAIA.
99 Secs 40 & 67 PAIA.
100 Secs 43 & 69 PAIA.
101 Sec 35 PAIA.
102 Sec 39 PAIA.
103 Sec 41 PAIA.
104 Sec 42 PAIA.
105 Sec 44 PAIA.
106 Sec 45 PAIA.
107 Secs 46 & 70 PAIA
108 As above.
109 ATI Act, http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%207M (accessed 14 August 2024).

Data Protection Act (DPA) became law in 2019.[110] The ATI Act similarly operationalises the right of access to information under article 35 of Kenya's Constitution. The formulation of article 35(1) is identical to that of South Africa's article 32(1). However, article 35 goes further to guarantee the right to 'the correction or deletion of untrue or misleading information that affects the person' and obligates the state to 'publish and publicise any important information affecting the nation.'[111]

Comparatively, the ATI Act's attempt to reconcile the competing interests on access to information and privacy, while not as elaborate as PAIA, is couched in similar themes. In rather broad terms, access to information shall be limited to protect national security; 'due process of law; the safety, health or life of a person'; unjustified privacy violation of another; substantial prejudice to the commercial interests of 'the data subject or a third party'; damage to a 'public entity's position in any actual or contemplated legal proceedings'; or professional confidentiality.[112] The ATI Act also provides a general public interest override requiring information disclosure by 'a public or private body where the public interest in information disclosure outweighs the harm to protected interests' subject to a court's determination.[113] Additionally, considerations of individual privacy and commercial interests do not apply 'if a request for information relates to the results of any product or environmental testing, and the information concerned reveals a serious public safety or environmental risk'.[114]

4.1 Judicial interpretation of the balance between access to information and privacy rights in South African and Kenyan courts

The legal systems in Kenya and South Africa are mixed, including both statute and common law pronouncements.[115] Common law is defined as law emanating from judicial decisions as opposed to statutes. In *Marbury v Madison* the United States Supreme Court stated: 'It is emphatically the province and duty of the judicial department to say what the law is. Those who apply the rule to particular cases, must of necessity expound and interpret that rule.'[116] Courts have a legal interpretive mandate that has been defined as 'the process or activity of using legal materials, such as statutes, constitutions, contracts, wills, and the like, to ascertain

110 DPA, http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20411C (accessed 14 August 2024).
111 Arts 35(2) & (3) Constitution of Kenya, https://kenyalaw.org/kl/fileadmin/pdfdownloads/TheConstitutionOfKenya.pdf (accessed 14 August 2024).
112 Secs 6(1)(d), (e), (h & (I) ATI Act.
113 Sec 6(4) ATI Act.
114 Sec 6(3) ATI Act.
115 WPR 'Common law countries 2024', https://worldpopulationreview.com/country-rankings/common-law-countries (accessed 14 August 2024).
116 *Marbury v Madison* 5 US 137, 177, 2 L Ed 60 (1803), https://supreme.justia.com/cases/federal/us/5/137/ (accessed 14 August 2024).

legal obligations, powers, rights, privileges, and so on'.[117] In other definitions, interpretation 'refers to the activity of the judge who, on the one hand, attempts to determine the scope of an ambiguous or obscure text and, on the other hand, attempts to elaborate a solution when the text presents a gap'.[118] South African and Kenyan courts have faced the task of dispelling the tensions in the statutory articulations of access to information and privacy rights in social contexts towards both determining the scope of the law, filling gaps and/or aligning the law to the spirit of the Constitution.

In *Arena Holdings* South Africa's Constitutional Court was confronted with a challenge to the constitutionality of the absolute exemption of taxpayer records from disclosure under section 35 of PAIA.[119] The case emanated from a refusal by SARS to accede to a 2019 request for the tax records of the former President, Jacob Zuma, following allegations that he evaded taxes during his tenure as President.[120] SARS denied the request because the records were confidential and exempted from disclosure as per sections 34(1) and 35(1) of PAIA, and section 69(1) of the Tax Administration Act (TAA).[121] The Court had a duty to balance the competing interests between the personal 'right to privacy of taxpayer records' against the public interest in accessing the records where there is evidence of serious illegality.[122]

The Constitutional Court had previously applied public interest considerations in ruling against the absolute prohibition of information disclosure on privacy grounds involving divorce proceedings[123] and asylum applications.[124] In confirming the order of the High Court on the unconstitutionality of the absolute prohibition under section 35 read together with section 46 of PAIA in *Arena Holdings*, the Constitutional Court asserted that the absolute exemption of individual tax records was not a less restrictive measure to limiting the right of disclosure.[125] The absolute approach contradicted the constitutional approach to competing rights. The Court added that applying the public interest override provided under section 46 of PAIA to the mandatory protection of taxpayer

117 M Greenberg 'Principles of legal interpretation' (2016), https://philosophy.ucla.edu/wp-content/uploads/2016/08/Principles-of-Legal-Interpretation-2016.pdf (accessed 14 August 2024).
118 A Rieg 'Judicial interpretation of written rules' (1979) 40 *Louisiana Law Review* 49. Also see F Geny *Method of interpretation and sources of private positive law* (1963).
119 *Arena Holdings (Pty) Limited t/a Financial Mail & Others v South African Revenue Service & Others* CCT365/21 (*Arena Holdings v SARS*) para 6, https://collections.concourt.org.za/bitstream/id/62514/[%20Judgment]%20CCT%20365-21%20Arena%20Holdings%20and%20Others%20v%20SARS%20and%20Others.pdf (accessed 14 August 2024).
120 As above.
121 *Arena Holdings* (n 119) para 7.
122 *Arena Holdings* (n 119) para 134.
123 *Johncom Media Investments Limited v M & Others* (CCT 08/08) [2009] ZACC 5; 2009 (4) SA 7 (CC); 2009 (8) BCLR 751 (CC) (17 March 2009), https://www.saflii.org/za/cases/ZACC/2009/5.pdf (accessed 14 August 2024).
124 *Mail and Guardian Media Ltd & Others v Chipu NO & Others* (CCT 136/12) [2013] ZACC 32; 2013 (11) BCLR 1259 (CC); 2013 (6) SA 367 (CC) (27 September 2013) paras 164 & 166, https://www.saflii.org/za/cases/ZACC/2013/32.html (accessed 14 August 2024).
125 *Arena Holdings* (n 119) para 171.

information would still ensure the protection of confidentiality as the disclosure would be limited and closely defined; the principle of severability would operate to demarcate the limits of disclosure; and the taxpayer would retain a right of notice, response and appeal.[126]

The order by the Constitutional Court in *Arena Holdings* not only obligated Parliament to address the constitutional conflict in the contentious provisions but went a step further in providing, in the interim, an amended wording to the contentious provisions that applies the public interest override to section 35 of PAIA's confidentiality provisions.[127]

Kenyan courts similarly have confronted questions on the privacy of taxpayers' records when faced with access to information demands in *Njoya*.[128] In the Court of Appeal case, the Kenya Revenue Authority (KRA) denied a request for information on whether members of parliament were paying taxes on the ground that it violated confidentiality under section 125 of the Income Tax Act.[129] The applicant challenged the constitutionality of the provisions with regard to article 35(1)(b) of the Constitution. In allowing the appeal, the Court of Appeal stated:[130]

> It is true to say that traditionally confidentiality of tax information is a globally recognised and accepted concept which is meant to be an aid in compliance ... Still, we entertain no doubt that the right to information is critical to the attainment of transparent and accountable government and is an enabler to the exercise and enjoyment of other rights by citizens. It has been recognised expressly in the Constitution of Kenya 2010, under article 35.

Notably, since the decision was made, the Income Tax Act was repealed by the Tax Procedures Act, effective as of January 2016.[131] Both events preceded the adoption of the ATI Act in Kenya. Two facts stand out: Unlike PAIA, the ATI Act does not expressly exempt the confidentiality of tax records from access to information requests under section 6. However, the Tax Procedures Act in stipulating exemptions to the confidentiality of taxpayer records excludes an information request that meets the public interest override standard.[132] It would be advisable for the Kenyan courts to learn from its South African counterparts in the provision of orders and provide further guidance to Parliament to cure the legislative anomaly where relevant. For example, South Africa's Constitutional

126 *Arena Holdings* (n 119) para 193.
127 *Arena Holdings* (n 119) paras 205(2) and (3).
128 *Timothy Njoya v Attorney General* Civil Appeal 112 of 2015 [2017] eKLR (*Njoya*), https://kenyalaw.org/caselaw/cases/view/141660/ (accessed 14 August 2024).
129 *Njoya* (n 128) 1. The Income Tax Act was replaced by the Tax Procedures Act 29 of 2015, http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20469B (accessed 14 August 2024). The confidentiality provisions and allowable exemptions are provided under sec 6.
130 *Njoya* (n 128) 5.
131 Act 29 of 2015, http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=CAP.%20469B (accessed 15 August 2024).
132 Sec 6 TPA.

Court amended the wording of the impugned provision pending parliamentary action. This allowed, on the one hand, guidance on a constitutionally aligned wording of the section and, on the other, protection of the doctrine of separation of powers.[133]

After the passage of the ATI Act, Kenyan courts have affirmed the importance of maximum disclosure in the interest of the public in light of section 6 exemptions that consider the right to privacy. In *Zebedeo John Opore v The Independent Electoral and Boundaries Commission*[134] the respondent denied an information request on certain information about a parliamentary seat election including the number of voters identified electronically, copies of polling station voter identification and verification forms, and polling station diaries. The IEBC rejected the request on grounds of privacy. However, in allowing the petition the High Court stated:[135]

> The fact that the information falls within the list of legitimate exception grounds is not sufficient to exempt it from disclosure. The disclosure must harm the specific interest substantially and this harm must be greater than the public interest in receiving the information. Disclosure takes precedence over secrecy, and to give effect to the principle of maximum disclosure, any legislation or provision contradicting this principle should be construed narrowly and in favour of the enforcement of the right.

In yet another case, *Tiso Blackstar Group (Pty) Ltd & Others v Steinhoff International Holdings NV*, the issue of legal privilege as a barrier to access to information was litigated at the Western Cape High Court.[136] The case arose from a refusal to honour an access to information request for an investigative report on accounting irregularities by the respondent, Steinhoff International Holdings NV, a public company. The applicants in this case are a media house and a civil society organisation. The public interest motivation behind the request was to accurately report on a public interest matter which, in this case, was the corporate scandal.[137] Access was denied on the grounds of legal privilege under section 67 of PAIA.[138] According to Steinhoff, the report that was the subject of the information request was prepared expressly to seek legal advice for actual or contemplated litigation. For a record to meet the test of litigation privilege, the document in question 'must have been obtained or brought into existence for the purpose of a litigant's submission to a legal advisor for legal advice; and second that litigation was pending or contemplated as likely at the time'.[139] In this

133 *Arena Holdings* (n 119) paras 205(2) and (3).
134 *Zebedeo John Opore v The Independent Electoral and Boundaries Commission* [2017] eKLR (*Opore*) para 39, http://kenyalaw.org/caselaw/cases/view/140609 (accessed 15 August 2024).
135 *Opore* (n 134) para 39.
136 *Tiso Blackstar Group (Pty) Ltd & Others v Steinhoff International Holdings NV* (18706/2019) [2022] ZAWCHC 265; 2023 (1) SA 283 (WCC) (10 May 2022) (*Blackstar*), https://www.saflii.org/za/cases/ZAWCHC/2022/265.html (accessed 15 August 2024).
137 *Blackstar* (n 136) para 10.
138 *Blackstar* (n 136) para 11.
139 *Competition Commission of South Africa v Arcerlormittal South Africa Ltd & Others* (680/12) [2013] ZASCA 84; [2013] 3 All SA 234 (SCA); 2013 (5) SA 538 (SCA); [2013] 1 CPLR

case, the respondent's claim of litigation privilege failed to meet the prescribed standard and the Court nullified the refusal.[140]

From the above selected cases, a trend emerges from Kenyan and South African courts to narrowly construe privacy restrictions when faced with a conflict with access to information in the interest of the public. This is especially so when the information is in the control of a public body, or a private body and necessary for the exercise of a right. Laudably, this is important towards promoting good governance, transparency and accountability in public and private institutions.

5 Conclusion

The quest towards finding the equilibrium between privacy and access to information is complex and multifaceted, requiring the intervention of legal frameworks at international, regional and domestic levels, and various enforcement actors including the judiciary. However, crucial instruments on the African continent, such as the African Commission's 2017 Guidelines on Access to Information and Elections in Africa, while impressively advancing access to information, have gaps with regard to the corresponding privacy and data protection rights. This article's analysis of the soft law instrument shows the importance of a holistic reading of international, regional and national law protections to balance access to information and privacy rights. South Africa and Kenya have made strides in confronting this rights conflict in their legal systems. Where a conflict emerges concerning balancing access to information and privacy, the laws and courts have underscored public interest disclosure considerations that supersede the potential harm of disclosure. Arguably, this approach, which eschews rights absolutism, allows for the better entrenchment of disclosure practices, good governance, accountability and transparency that has historically marred national democratic trajectories in African countries.

1 (SCA) (31 May 2013) para 21, https://www.saflii.org/za/cases/ZASCA/2013/84.html (accessed 15 August 2024).

140 *Blackstar* (n 136) para 70.

African Journal on Privacy & Data Protection

To cite: O Babalola 'The constitutional origins of the right to privacy in Nigeria' (2025) 2 *African Journal on Privacy & Data Protection* 83-97
https://doi.org/10.29053/ajpdp.v2i1.0005

The constitutional origins of the right to privacy in Nigeria

*Olumide Babalola**
PhD Researcher, University of Portsmouth, United Kingdom

Abstract

The right to privacy – a fundamental right and tortious claim – has its deep historical roots traceable to the academic advocacy of Warren and Brandeis in their 1890 article published in the Harvard Law Review. The article closely or remotely invokes the characteristic propensity for judicial activism by the American courts towards the enforcement of the right even though empirical evidence exists on the judicial recognition on privacy in the eighteenth century. In the Nigerian context, even though it is sparingly recorded that the evolution of privacy has been influenced by a myriad of factors, including minority agitation, colonial legacies, political machinations and contemporary legal developments, this article represents an academic ascertainment of the origins of privacy as a fundamental right in Nigeria by tracing its historical trajectory from precolonial constitutional conference proceedings. Combining a predominantly descriptive legal historical methodology with a touch of analytic review, the article emphasises some 'semantic' inconsistencies in the few existing academic accounts of the entry of privacy into the Nigerian pre-colonial and Independence Constitutions. By reviewing relevant case law on privacy and the authoritative constitutional documents, the article concludes that, contrary to the repeated

* PhD Researcher, University of Portsmouth, UK; Chair, Nigerian Bar Association's Data Protection Committee. olumide.babalola@port.ac.uk

academic statements fixing the entry of privacy to the Nigerian Independence Constitution, privacy in Nigeria has been constitutionally recognised as an appendage to the 1954 (Lyttleton) Constitution.

Key words: Constitution, privacy, Nigeria, origin, right

1 Introduction

Internationally, privacy,[1] unlike other fundamental rights, did not become a human right through national constitutions. Diggleman and others discovered that '[t]he right to privacy became an international human right before it was a nationally well-established fundamental right'.[2] In Nigeria, academic discourse around the concept of privacy and its variants, whether as a right or object of entitlement, continues to flow along the lines of socio-legal realities, but the historical context has been palpably ignored. The few Nigerian academic papers bearing historical accounts on the origin of privacy are all focused on its American trajectories, thereby completely blotting out the eventful moments ushering in the right in the pre- and post-colonial Nigerian constitutional documents.

Without attempting to rewrite history, this article identifies the scant but direct literature on the origins of the right to privacy in Nigeria. This is particularly done by sieving privacy out of the Bill of Rights – the subject matter of the historical literature. With a predominantly descriptive method, the article references earlier literature tracing the origins of privacy in Nigeria, illuminating the characters and events that influenced the inclusion of bills of rights in the pre-colonial and Independence Constitution and the source of such inspiration. On choice of methodology for historical legal research of this sort, Majeed notes that

> similarly, the fourth step of his methodology is concerned with addressing the hypothesis or research questions and putting forward the conclusions about them. All this requires certain tasks to be performed which include checking the historical facts, evaluation of the validity and reliability of collected data and analysis of the evidence collected from various sources.[3]

The last step of Majeed's methodology is about the report writing which involves description and interpretation of findings. From the minority agitations to the whimsical political shenanigans culminating in the constitutional frameworks on privacy, the article navigates through the labyrinth of history to unravel the entry of the right to privacy in Nigeria's constitutional arrangement.

1 The right to privacy is advisedly used interchangeably with 'privacy' in this article. The distinction between the two concepts has been likened to an analogy of the chicken and its egg. While the right to privacy is a legal entitlement, privacy is the object of that entitlement. See O Babalola *Privacy and data protection law in Nigeria* (2021) 9.

2 O Diggelmann & MN Cleis 'How the right to privacy became a human right' (2014) 14 *Human Rights Law Review* 441.

3 N Majeed, A Hilal & R Ilyas 'On historical and historical-legal research: Forms, challenges and methodologies' (2023) 5 *Pakistan Journal of Social Research* 528.

For clarity, the article is divided into six parts. The first part introduces the subject of discourse and the next part justifies the necessity, while the third part reproduces the definition of privacy as provided by Nigerian academics and jurists. The fourth part analyses the inconsistent historical accounts of the origin of the right to privacy in Nigeria, and the fifth part emphasises the oft-ignored nexus between privacy as known in Nigeria and the European Charter on Human Rights (European Charter). The last part concludes with a brief recap of the discourse.

2 Rationale of this contribution

In my doctoral research, it became imperative to interrogate the cultural relativity of privacy (beliefs) in Nigeria and that led to a finding of the European influence on the inclusion of human rights in the Nigerian (pre-colonial) Constitution and Independence Constitution. The origin of fundamental rights (privacy inclusive) is palpably omitted from many existing academic contributions on human rights in Nigeria. As far back as 1965, Amachree observed this, and the situation has not changed. He notes:[4]

> The fundamental rights provisions in the Nigerian Constitution have, as is to be expected, afforded jurists an opportunity to produce learned legal articles and commentaries. The majority of the writers and commentators have, however, dealt more with the legal interpretation of the provisions than with the historical background.

Most Nigerian academics simplistically allude to international bills of rights as the 'source' of fundamental rights without more. Conversely, the few accounts of the origin of fundamental rights in Nigeria are at loggerheads. Hence, there is an imminent need for legal historical clarity in this regard. On the importance of legal history, Phillips argues that such a study establishes legal contingency, that is, law exists within human societies.[5] From a Nigerian perspective, this may help push the relatable narrative of cultural relativism with regard to privacy beliefs in Nigerian societies. From the foregoing, this article becomes essential for two reasons: first, to resolve the existing conflict with documentary evidence; and, second, it represents the first academic paper solely dedicated to the origin of privacy in Nigeria – the earlier ones are focused on fundamental rights as a bundle.[6]

4 GKJ Amachree, 'Fundamental rights in Nigeria' (1965) 11 *Howard Law Journal* 463.
5 J Phillips 'Why legal history matters' (2010) 41 *Victoria University of Wellington Law Review* 293.
6 These are considered later in the article.

3 Defining of privacy: The Nigerian way

Universally, privacy remains an elusive concept to define.[7] Regardless of the lack of consensus on its definition, many researchers have attempted to define or describe the concept from multicultural perspectives.[8] From a theoretical perspective, it is important to define the notion of privacy for many reasons. First, the definition gives clear insight into the core and essential functionality of the concept as distinguished from other related interests.[9] Then such offers an unmistakable foundation for the understanding and application of legal frameworks for redress, thereby eliminating a conflation of concepts. Defining the rigours of privacy also helps an appreciation of its cultural relativism, thereby giving effect to all the diverse interests protected by the notion. Despite the relatively low quantity of literature on the right to privacy in Nigeria, some authors and jurists have, at varying times, defined privacy from diverse perspectives. While resolving a dispute on bodily integrity, the Nigerian Supreme defined the concept as 'a right to protect one's thought, conscience or religious belief and practice from coercive and unjustified intrusion; and, one's body from unauthorised invasion'.[10] This definition is rather narrow as it omits elements of spatial privacy, information privacy, publication of private facts and publicity in a false light, and so forth. In another decision, the High Court of Lagos State defined privacy as 'the presumption that individuals should have an area of autonomous development, interaction and liberty a "private sphere" with or without interaction with others, free from arbitrary state intervention by other uninvited individuals'.[11] This definition also focuses on non-interference with seclusion – a passive aspect of privacy – in total disregard of the active version where an individual assumes control over and decides who has access to their privacy spheres.[12]

Nigerian academics have also attempted varying definitions of the notion of privacy. Nwauche believes that privacy is better described that defined and that the lack of a universally-acceptable definition does not detract from the dynamism and development of privacy. He restrictively describes it as the legal

7 A Alibeigi, AB Munir & nd MD Ershadul Karim 'Right to privacy, a complicated concept to review' (2019) *Library Philosophy and Practice* 2841.

8 For some definitions of privacy, see T Dixon 'Valuing privacy: An overview and introduction' (2001) 39 *Journal of Social Philosophy* 411; AD Moore 'Defining privacy' (2008) 39 *Journal of Social Philosophy* 411; EVD Haag 'On privacy' in JR Pennock & JW Chapman (eds) *Privacy* (1971) 56; R Gavison 'Privacy and the limits of law' (1980) 89 *Yale Law Journal* 423; A Westin 'Privacy and freedom' (1968) 25 *Washington and Lee Law Review* 166; C Fried 'Privacy' (1968) 77 *Yale Law Journal* 482; T Gerety 'Redefining privacy' (1977) 12 *Harvard Civil Rights-Civil Liberties Law Review* 281.

9 DK Mulligan, C Koopman & N Doty 'Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy' (2016) 374 *Philosophical Transactions. Series A, 20160118*.

10 *Medical Dental Practitioners Disciplinary Tribunal v Dr John Okonkwo* (2001) 7 NWLR (Pt 711) 206.

11 Unreported Suit LD/14895MFHR/2023 between Olumide Babalola and Oyinlola Adebayo delivered by Hon Justice OA Oresanya (Mr) on 13 February 2024.

12 SS Al-Fedaghi 'The right to be let alone and private information' in C Chen and others (eds) *Enterprise information systems VII* (2006) 117.

right that allows an individual to lead their desired life devoid of interference,[13] but expansively considers other issues surrounding the notion. In a simplistic manner, Olomojobi addresses the notion of privacy in the realm of information or human activities intended to be restricted or excluded from others' knowledge,[14] but elucidates further that the right protects and individual's affairs from the prying eyes of the public.[15]

Privacy has also been described or defined as the right or condition of being protected from unjustifiable, undesired or unauthorised observation, intrusion, or interference into an individual's personal affairs. This right effectively ensures that individuals have considerable reasonable control over their personal choices, information, decisions and spaces, ensuring that they can choose what personal information to divulge, with whom, and under what circumstances.

In their technology-focused paper, Abdulrauf and Daibu conceptualise privacy in the context of spatial protection of an individual's home, physical space and property. According to the authors, privacy predominantly concerns the protection of individuals from intrusion into their private or family life.[16] By their attempt, the learned authors conclude that, with the ubiquity of technology, the contemporary definition of privacy ought to accommodate all the peculiar concerns of the phenomenon. After a disclaimer against proposing an all-encompassing definition, Babalola defines privacy as 'a fundamental right protection afforded a natural person from undesired or unauthorised interference with his/her personal affairs or relationships by whatever means irrespective of the purpose',[17] while Salau defines the concept in terms of a passive right which entitles an individual within any given society to reasonable expect that his personal affairs are protected from 'patronising, paternalistic or meddlesome influences by others'.[18] Regardless of the attempts by Nigerian academics, a universally-acceptable definition still eludes the concept of privacy. However, understanding the notion from a cultural relativism perspective holds the potential for peculiar development of the concept in Nigeria.

13 ES Nwauche 'The right to privacy in Nigeria' (2007) 1 *CALS Review of Nigerian Law and Practice* 63.
14 Y Olomojobi 'Right to privacy in Nigeria' in O Babalola & K Okwujiako (eds) *Emerging jurisprudence on privacy and data protection in Nigeria* (2023) 3.
15 As above.
16 LA Abdulrauf & AA Daibu 'New technologies and the right to privacy in Nigeria: Evaluating the tension between traditional and modern conceptions' (2016) 7 *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 113.
17 Babalola (n 1) 17.
18 AO Salau 'Cybersecurity, state surveillance and the right to online privacy in Nigeria: A call for synergy of law and policy' (2024) 1 *African Journal on Privacy and Data Protection* 152-175.

4 Conflicting accounts of the origin of privacy in Nigeria

It cannot be overemphasised that the literature on the right to privacy in Nigeria remains scanty despite a remarkable increase in recent times.[19] Seven years after Salau's[20] and Odusote's[21] observations on privacy as the most under-researched fundamental right by Nigerian academics, not much has changed, as evidenced by the existing literature on the subject. For example, Nwabueze – fondly remembered as the father of constitutional law in Nigeria – clearly accounts for 1958 as the entry of fundamental rights into our constitution thus: 'On the recommendation of the Minorities Commission in 1958, a guarantee of fundamental right was incorporated into the Constitution in that year and was retained in both 1960 and 1963 Constitutions. The guaranteed rights were ... private and family life.'[22]

Remarkably, Mowoe's[23] and Hon's[24] expositions on the right to privacy are quite extensive but, unfortunately, omit an account of the origins of the right in Nigeria. Both learned authors discuss privacy only from section 37 of the 1999 Constitution without any historical flavour. Oluyede,[25] Oyewo,[26] Susu[27] and Malemi[28] completely avoid a historical account of how fundamental rights were introduced into the Nigerian Constitution – an academic omission with a long history of 'culprits' as noted by Amachree thus: 'The fundamental rights provisions in the Nigerian Constitution have, as is to be expected, afforded jurists an opportunity to produce learned legal articles and commentaries.' The majority of the writers and commentators have, however, dealt more with the legal interpretation of the provisions than with the historical background. One writer, in an otherwise very informative article, had no more to say on the history of the provisions than that recounting how the Willink Commission recommended the inclusion of fundamental rights as a panacea to pacifying the minorities' fears during the pre-independence agitations.[29] Other writers

19 Early in 2024 I compiled a bibliography of academic articles on the right to privacy and data protection listing a total of 126 articles. See O Babalola 'Data protection and the right to privacy in Nigeria: A bibliography', https://papers.ssrn.com/abstract=4625918 (accessed 2 June 2024).

20 AO Salau 'Data protection in an emerging digital economy: The case of Nigerian Communications Commission: Regulation without predictability' (2016) Broadening the Horizons of Information Law and Ethics: A Time for Inclusion 1.

21 A Odusote 'Data misuse, data theft and data protection in Nigeria: A call for a more robust and more effective legislation' (2021) 12 *Beijing Law Review* 1284.its influence on global systems and economies, and the harm that may arise from its abuse. This makes data protection laws important to protect the privacy data subjects all over the world, which is a fundamental human right under article 12 of the Universal Declaration of Human Rights (UDHR, 1948

22 B Nwabueze *A constitutional history of Nigeria* (1982) 116.

23 KM Mowoe *Constitutional law in Nigeria* (2008) 405.

24 ST Hon *ST Hon's constitutional and migration law in Nigeria* (2016) 535.

25 P Oluyede *Constitutional law in Nigeria* (1992) 23.

26 O Oyewo *Constitutional law in Nigeria* (2020).

27 B Susu *Constitutional litigation in Nigeria* (1999).

28 E Malemi *The Nigerian constitutional law* (2012).

29 L Izuagie 'The Willink Minority Commission and minority rights in Nigeria' (2015) 5 *Ekpoma Journal of Theatre and Media Arts* 206.

have tended to explain the background by very brief references to minority fears without giving any details as to what those fears were.[30] Happily, Amachree seems to have academically plugged the historical gap by emphatically fixing the entry of fundamental rights into Nigerian law through the 1960 Constitution:[31]

> At the Constitutional Conference held in London in May and June 1957, it was agreed that provisions should be made in the Independence Constitution for fundamental rights ... These clauses were to be submitted to the governments of the different regions of Nigeria and were to be considered at the resumed Conference held in London in September and October of 1958 ... The Commission divided the fundamental rights into five groups which they recommended should be included in the Constitution. These were ... (5) private and family life ... These recommendations are based on articles 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14 of the European Convention on Human Rights and on article 9(2) of the Malaya Constitution which deals with freedom of movement, and article 13(1) and (2) of the Pakistan Constitution from which the provisions pertaining to religious education were obtained. The recommendations were adopted and incorporated in the (1960) Constitution as chapter III.

This academic account was later judicially confirmed in Darman's case[32] where Karibi-Whyte[33] notes thus:[34]

> Before examining the arguments before the court, particularly concerning the jurisdiction of the court, it is relevant in this judgment to explain even if superficially the origin and nature and constitutional status of the action now known as fundamental right ...The earliest attempt to incorporate fundamental rights in the Constitution was at the 1957 Constitutional Conference, when the Action Group ... requested the addition of a set of fundamental rights in the Constitution ... It however went on to recommend the entrenchment in the Constitution of fundamental rights as a safeguard for minorities, as a check against the abuse of majority power. Its detailed proposals followed closely the terms of the European Convention on Human Rights, adopted by the United Kingdom parliament barely eight years previously. These proposals were substantially approved by the Constitutional Conference of 1958.

Although in the appendix to Amachree's paper, reference is made to pre-1960 court cases litigated on fundamental rights, the account in the body of the paper somewhat gives a confusing narrative that fundamental mental rights originated from the 1960 Independence Constitution. This could have swayed the Court of Appeal's emphatic statement that 'the earliest attempt' to incorporate fundamental rights into a constitution was in 1957.[35]

30 Amachree (n 4) 528.
31 As above.
32 *Federal Minister of Internal Affairs v Shugaba Abdulrahman Darman* (1982) 2 NCLR 915.
33 Justice of the Court of Appeal (as he then was).
34 As above.
35 As above.

In Parkinson's account, a suggestion for the inclusion of fundamental rights in the Constitution was rejected during the constitutional conference in 1953. By his graphic narration:[36]

> When Awolowo raised the issue of fundamental rights at the conference in 1953, the Secretary of State for the Colonies ridiculed a bill of rights out of serious consideration by saying that the Nigerians could put 'God is Love' into their constitution if they so wished, but not while he was chairing the conference. This stance reflected the orthodox Colonial Office position on bills of rights in colonial constitutions, namely that such instruments are of little value and were unknown in British colonial constitutions. The resulting Lyttleton Constitution, named after Oliver Lyttleton, the Secretary of State for the Colonies, came into operation in September 1954.

For unknown reasons, Parkinson's account, however, omits to acknowledge the provisions of fundamental rights in the schedule to the 1954 Lyttleton Constitution with his statement that

> [t]he foreshadowed next constitutional conference was set to commence on May 23, 1957 ... The question of a bill of rights was again raised at the conference ... Since the 1953 Constitutional Conference, the Colonial Office had reviewed its policy on colonial bills of rights and, in a fundamental policy shift, changed its position from total opposition to a bill of rights in any colonial constitution to limited support for a bill of rights for Nigeria's independence constitution.[37]

On the same wavelength, Ediagbonya also traces the entry of fundamental rights to the Independence Constitution thus:[38]

> On the controversial issue of the fears of the minority groups in the country based on the recommendation of the Minority Commission that no state should be created instead fundamental human rights should be entrenched in the constitution. The conference agreed that a number of rights and freedom like the right to life, the right to religion, the freedom of peaceful assembly, movement, speech, association etc should be entrenched in the constitution of the Federal Republic of Nigeria. So the conference accepted the inclusion of a long list of fundamental human rights in the constitution to protect Nigerian citizens (majority and minority alike) against arbitrary abuse of power by government (Report by the Resumed Nigeria Constitutional Conference (1958).

The foregoing accounts, including those of Proehl[39] and Seng,[40] all point to the conclusion that privacy surfaced for the first time in the 1960 Independence Constitution, but such a conclusion is not failproof when other academic or judicial accounts are considered. For example, Gledhill declares that 'fundamental human rights have now been written into the Nigerian Constitution, and the first

36 C Parkinson *Bills of rights and decolonisation: The emergence of domestic human rights instruments in Britain's overseas territories* (2008) 539.
37 As above.
38 M Ediagbonya 'Nigeria constitutional development in historical perspective, 1914-1960' (2020) 4 *American Journal of Humanities and Social Sciences Research* 242-248.
39 PO Proehl *Fundamental rights under the Nigerian Constitution, 1960-1965* (1970) 1.
40 MP Seng 'Democracy in Nigeria' (1985) 9 *National Black Law Journal* 113.

two decisions involving fundamental rights in Nigeria, both from the Northern Region High Court, have recently come to hand'.[41] In the article published by the School of Oriental and African Studies in the summer of 1960, the author reviews two decisions[42] filed for the enforcement of the right to privacy (among other fundamental rights) in 1959 before the Independence Constitution. The cases were litigated pursuant to the fundamental rights contained in the schedules to the Nigeria (Constitution) Order in Council 1954, thereby showing a conflict in the academic reports that fundamental rights originated from the 1960 Independence Constitution.

In what turns out to be a legal historical ice breaker, Vasak copiously reports:[43]

> Presided over by Sir Henry Willink, the Minorities Commission submitted its report in July 1958. It pronounced against the creation of new regions and proposed, as one means of allaying the fears of the minorities, the inclusion in the Nigerian Constitution of provisions guaranteeing certain fundamental rights. In the view of the Commission: 'Provisions of this kind in the Constitution are difficult to enforce and sometimes difficult to interpret. Nevertheless, we think they should be inserted. Their presence defines beliefs widespread among democratic countries and provides a standard to which appeal may be made by those whose rights are infringed ... We have therefore considered what provisions might suitably be inserted in the Constitution and have given particular attention to the Convention on Human Rights to which, we understand, Her Majesty's Government has adhered on behalf of the Nigerian Government.' On the basis of the proposals of the Minorities Commission the Colonial Secretary of the United Kingdom prepared a draft text, which was presented to the Constitutional Conference of September and October 1958 in London. This Conference prepared a text and recommended its inclusion in what was to be the Independence Constitution. However, at the request of the Nigerian political leaders, the Chapter relating to human rights was promulgated even before independence on October 24, 1959, that is to say, before the federal elections which took place on December 18, 1959. For the Nigerian leaders, indeed, it was during the electoral period that respect for human rights became absolutely essential ...These provisions were published as the Sixth Schedule to the Constitutional Order of 1954. In the Constitution of independent Nigeria, which came into force on October 1, 1960, the provisions of the Sixth Schedule were repeated with a few minor amendments as Chapter III (Fundamental Rights) of the Second Part of the Constitution of the Federation of Nigeria.

This comprehensive account remarkably closes the gap identified in other accounts, especially on the reconciliation between the provision of privacy (bills of rights) in the 1954 Constitution and the regurgitated statements that fundamental rights originated from the 1960 Constitution. It is more plausible,

41 A Gledhill 'Fundamental rights in Northern Nigeria' (1960) 4 *Journal of African Law* 115.
42 Unreported Suit K/M26/1959) between Dahiru Cheranci and Alkali Cheranci; unreported Suit Z/22/1959 between J Olawoyin and Attorney General, Northern Region. This case is analysed later in this article. See also DL Grove 'The "sentinels" of liberty? The Nigerian judiciary and fundamental rights' (1963) 7 *Journal of African Law* 152.
43 K Vasak 'The European Convention of Human Rights beyond the frontiers of Europe' (1963) 12 *International and Comparative Law Quarterly* 1206.

from a historical perspective, to understand that, even though agitations for the inclusion of fundamental rights were directed towards the Independence Constitution of 1960, the politicians succeeded in making fundamental rights an appendage to the existing 1954 Constitution at the tail end of 1959. Hence, to clear the air, irrespective of the motive or narrative, fundamental rights are clearly provided under the schedule to the 1954 (Lyttleton) Constitution and the Nigerian Supreme Court has repeatedly held that schedules to an Act/ Statute are part of the legislation,[44] hence a categorical statement or suggestion that the fundamental rights surfaced for the first time in Nigeria in the 1960 Independence Constitution is misleading.

5 Source(s) of the right to privacy and the European Charter influence

The Nigerian literature is replete with academic narrations on the sources of the Nigerian law or legal system. Like many other academic commentators on the issue, Park,[45] Obilade,[46] Alkali,[47] Gwangndi,[48] Nwalimu[49]and Alabi[50] all identify received English law, common law, customary law and case law as the major sources of Nigerian law. However, a distinct narration on the 'source' of privacy is missing from the existing literature as it is usually taken for granted that the common international instruments are the sources of Nigeria's bills of rights. For example, the Universal Declaration of Human Rights (Universal Declaration) and the International Covenant on Civil and Political Rights (ICCPR) have enjoyed a large chunk of academic attention in most of the discourse on the sources of fundamental rights in Nigeria.[51]

44 *Dr Olusola Saraki v Federal Republic of Nigeria* (2016) LPELR – 40013(SC); *NNPC v Famfa Oil Ltd* (2012) 17 NWLR (Pt 1328) 148.
45 AEW Park *The sources of Nigerian law* (1963).
46 AO Obilade *The Nigerian legal system* (1979).
47 AU Akali and others 'Nature and sources of Nigerian legal system: An exorcism of a wrong notion' (2014) 5 *International Journal of Business, Economics and Law* 1.
48 MI Gwangndi 'The socio-legal context of the Nigerian legal system and the Shariah controversy: An analysis of its impact on some aspects of Nigerian women's rights' (2016) 45 *Journal of Law, Policy and Globalisation* 1.
49 C Nwalimu *Nigerian legal system* (2008).
50 LA Ayinla 'Jurisprudential perspectives on the fountain of Nigeria legal system' (2020) 13 *Agora International Journal of Juridical Sciences* 15-24.
51 See EA Odike & A Akujobi 'Enforcement of fundamental rights in national constitutions: Resolving the conflict of jurisdiction between the Federal High Court and State High Court in Nigeria' (2018) 9 *Beijing Law Review* 53; NO Anyadike, ST Nwachukwu & JO Wogu 'Human rights in Nigeria and the implications of human rights education for resource collection by libraries' (2021) *Library Philosophy and Practice* 5391; AS Fadlalla 'Fundamental rights and the Nigerian draft constitution' (1977) 10 *Verfassung in Recht und Übersee* 543; E Taiwo 'Enforcement of fundamental rights and the standing rules under the Nigerian Constitution : A need for a more liberal provision' (2009) 9 *African Human Rights Law Journal* 548; H Hannum 'The status of the Universal Declaration of Human Rights in national and international Law' (2014) 25 *Georgia Journal of International and Comparative Law* 287.

Surprisingly, within and outside the Nigerian classrooms, the direct and exclusive inspiration of the contents and wording of fundamental rights in the Nigerian Constitution has not been befittingly discoursed.

Commenting on the 'content' of (fundamental) rights in the context of the constitutional provision as contained in the Independence Constitution, Nwabueze overlooked the documents that provided a precedent for the draftsmen but deflected to the relic of colonialism thus:[52]

> But the content of a constitutional guarantee of rights depends not only upon the range of rights guaranteed but also upon the scope and sweep of the qualifications made to them ... In spite of these deficiencies of the guarantee, its incorporation in the Nigerian Constitution was a major development in the country's constitutional history. Of Britain's legacies to the country, perhaps the most valuable is the libertarian tradition of the common law and its system of justice. Resting upon a *laissez-faire* conception of society, the common law has a zealous concern for private rights, not only civil and political liberty but individual freedom of action generally. It is the tradition of British justice, said Lord Atkin, that judges should not shrink from upholding the lawful rights of the individual in the face of the executive.

Nwabueze's fixation on the common law as reproduced above is flawed for two reasons. Neither the common law nor the British legal system played any role in shaping the contents or wording of Nigeria's Bill of Rights. Second, the United Kingdom had no relatable or influential fundamental rights framework that could offer some form of precedent to Nigeria at all material times since the 1689 English bills of rights predominantly guarantee basic civil rights and royal succession – a non-binding[53] and insignificant document to the guarantee of fundamental rights.[54] In this same respect, it also is worthy of note that, at Nigeria's independence, Britain neither had fundamental rights written in its Constitution nor a statute dedicated to fundamental rights – the extant Human Rights Act was passed in 1998.[55]

In an unprecedented manner, Amachree – the only Nigerian to have done so at the time – traces the transplantation of the right to privacy into the Nigerian Constitution from the European Convention on Human Rights (European Convention) thus:[56]

> At the Constitutional Conference held in London in May and June 1957, it was agreed that provisions should be made in the Independence Constitution for fundamental rights ...The wishes of the Conference were duly carried out ... It is felt in spite of the wide terms of reference of the Com- mission that they

52 Nwabueze (n 9) 118.
53 A Lester 'Fundamental rights in the United Kingdom: The law and the British Constitution' (1976) 125 *University of Pennsylvania Law Review* 337.
54 P Murrell 'Design and evolution in institutional development: The insignificance of the English Bill of Rights' (2017) 45 *Journal of Comparative Economics* 36.
55 R Costigan & PA Thomas 'The Human Rights Act: A view from below' (2005) 32 *Journal of Law and Society* 51.
56 Amachree (n 4) 528.

> may have been averse to the inclusion of any fundamental rights in the Nigerian Constitution ... However, as it was part of their duty to propose means of allaying the fears of minorities and to make recommendations as to the safeguards to be included in the Constitution, the Commission accepted the proposal by the church groups. The Commission divided the fundamental rights into five groups which they recommended should be included in the Constitution. These were ... private and family life ... These recommendations are based on articles 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13 and 14 of the European Convention on Human Rights ... The recommendations were adopted and incorporated in the Constitution as Chapter III.

The foregoing narration shows in clear terms that the privacy under the Nigerian Constitution was fashioned after its European counterpart from where inspiration was drawn.

In a more graphic relation of the verbatim transplantation of the European Convention as Nigeria's bills of rights, Vasak recounts thus: 'The Nigerian Constitution guarantees the following rights, whose definitions for the most part have been taken almost word for word from the European Convention ... right to respect for private and family life, home and correspondence (article 22; cf article 8 of the Convention.'[57] Confirming the European Convention as the identical source of the right to privacy in Nigeria, Parkinson narrates:[58]

> The methodology of the Nigeria Working Group was to cut and paste a bill of rights from various sources. Eastwood later described the approach of the Nigeria Working Group to preparing the draft bill of rights in a minute: 'We have taken the European Convention (to which Nigeria adheres) as a model ... As the European Convention on Human Rights was the most comprehensive bill of rights then drafted with the input of British lawyers, it necessarily formed the backbone of the list, being used in fourteen of the eighteen sections.

In De Smith's intervention, rather than credit the constitutional debut of privacy to minority groups, he ascribes it to political whims and strategy thus:[59]

> The full story of the Nigerian constitutional conferences preceding independence has yet to be written, but it is believed that the origins of the decision to incorporate fundamental rights in the Constitution are directly traceable to local politics ... At the 1957 Constitutional Conference the Government of the Western Region sponsored two proposals that would have tended to weaken the position of the NPC: the creation of a small number of new States (which would diminish the size of the Northern Region) the adoption of a set of fundamental rights (which might affect the policies pursued by the N.P.C. and make it easier for its opponents to organise freely in the North) ... The Minorities Commission came to the conclusion that the case for new States had not been made out. It discovered little enthusiasm in Nigeria for the entrenchment of fundamental rights as a guard for minorities; nevertheless, it recommended that it be written into the Constitution together

57 Vasak (n 29) 1217.
58 Parkinson (n 22) 554.
59 SA de Smith 'Fundamental rights in the new Commonwealth – II' (1961) 10 *International and Comparative Law Quarterly* 215.

> with other checks against the abuse of power. Its detailed proposals closely followed the terms of the European Convention on Human Rights (the Convention for the Protection of Human Rights and Fundamental and Freedoms, 1950) ... These recommendations were substantially approved at the Constitutional Conference held in 1959.

According to Proehl,

> the 1960 Bill of Rights of the Nigerian Constitution came about because the Minorities Commission Report of 1958 had recommended that the fears of minorities, into which the Commission had inquired, would be allayed by express constitutional guarantees of rights. These were to follow the European Convention for the Protection of Human Rights and Fundamental Freedoms. The convention had already been adhered to by the British Government on behalf of Nigeria, but to have the force of law in Nigeria, it had first to become part of Nigerian municipal law. This is well known, but it is worth noting that the traditional British reserve against the inclusion of ex-press fundamental rights in the constitutions of its colonial or former colonial territories was now laid aside in favour of such incorporation, but not without misgivings.[60]

Narrating from a colonial heritage perspective, Seng accounts:[61]

> One of the final acts of the colonial government prior to independence was to bequeath to Nigeria a Bill of Rights. The Bill of Rights was recommended by the Minorities Commission appointed in 1957 to study the problems of minority tribes in the three regions. Rather than recommending the creation of new states ... the commission suggested the inclusion of a bill of rights into the constitution. The Bill of Rights did not solve the problems of the minority tribes, but it has formed the model for the protection of individual rights in all subsequent constitutions. The Bill of Rights was patterned after the European Convention on Human Rights ... It also had provisions guaranteeing ... the rights of privacy and family life.

Despite the existing academic accounts of the European Convention's influence on the contents and wording of the constitutional right to privacy in Nigeria, contemporary writings conspicuously omit this very important historical connection. Surprisingly, with the exception of Babalola[62] who made slight allusion to the Convention's influence on the inclusion of 'private and family life' in the wording of the provision, earlier writers such as Nwauche,[63] Olomojobi,[64]

60 Proehl (n 37) 1.
61 Seng (n 38) 113.
62 Here I simply note that '[t]he phrase "private and family life" was likely copied from article 8 of the European Convention on Human Rights which was adopted in 1948 – twelve years before Nigeria's Independence Constitution was drafted in 1960'. In a related context, I continue on page 109 that '[m]ost of the definitions adopted in the NDPA are verbatim (or with slight modifications) reproductions of the definitions in the GDPR thereby giving further credence to the submission that European law in part of the source of data protection in Nigeria'. See Babalola (n 1) 38 & 109.
63 Nwauche (n 13) 63.
64 Olomojobi (n 14) 3.

Abdulrauf[65] and Adekunle,[66] who have all written relatively comprehensive pieces on the concept of privacy, inexplicably avoid this historical root.

Identifying the European link to Nigerian privacy is essential for many reasons. Since there exists a clear distinction between the European and American approaches to privacy, it is imperative for Nigeria to know what pattern to follow or draw lessons from together with the justification of such choice. For context, in Europe, privacy is rights-based;[67] hence, the clear guarantees in the international treaties and national constitutions, but in the US, privacy is an expectation-based concept developed as a tort. This potential conflation of approaches appears in some Nigerian literature without necessary clarification of the divergent jurisdictional preferences and what it portends for Nigeria. Nwauche, the foremost author on the subject, notes:[68]

> An idea of the key issues in the right to privacy can be found in the classification of the jurist Prosser of the four torts which had then emerged from the American protection of privacy. These four torts are: (i) publicity which places plaintiff in a false light; (ii) appropriation of the plaintiff's name or likeness; (iii) intrusion upon plaintiff's seclusion or solitude; and (iv) public disclosure of private facts about the plaintiff. Even though these torts have found different manifestations in different countries, they remain the signposts for the protection of the right to privacy.

Surprisingly, despite identifying the right-based provision of privacy under the Nigerian Constitution, Nwauche does not acknowledge the converse provision of privacy as a tort under another existing Nigerian legislation, and this omission is repeated by Abdulrauf and Daibu when they argue that '[u]nlike the common law of England, the common law applicable in Nigeria does not recognize an independent tort of privacy. What is applicable in Nigeria is an equitable action of breach of confidence.'[69] While the statement is not wrong, the authors, however, missed an opportunity to analyse the multi-jurisdictional approach (that is, rights-based and civil wrong) Nigeria has taken to privacy as evidenced by the provision of Law Reform (Torts) Law thus:[70]

> (1) Anyone who intentionally intrudes, physically or otherwise, on the solitude or seclusion of another or private affairs or concerns, is liable for invasion of privacy, if the intrusion would be highly offensive to a reasonable person.
> (2) Anyone who uses the name or likeness of another in a manner and to an extent which suggests to a reasonable person an intention to appropriate the name and likeness of another or that is associated with another is liable to damages.

65 Abdulrauf & Daibu (n 16) 113.
66 A Adekunle & I Okukpon 'The right to privacy and law enforcement: Lessons for the Nigerian judiciary' (2017) 7 *International Data Privacy Law* 202.
67 D Buresh 'A comparison between the European and the American approaches to privacy' (2021) 6 *Indonesian Journal of International Law* 253.
68 Nwauche (n 13) 63.
69 Abdulrauf & Daibu (n 16) 113.
70 Sec 29 Law Reform (Torts) Law Ch L82, Laws of Lagos State 2015.

(3) Anyone who publicizes a matter concerning the private life of another is liable for invasion of privacy.

Even though no reported cases exist where the provision has been interpreted or enforced, it remains part of Nigeria's *corpus juris* and confirms the multi-jurisdictional approach to privacy that robs Nigeria of a clearly-identifiable methodology, the theoretical development of the right to privacy.

6 Conclusion

In this article I have analysed the necessity of identifying the origins and sources of the right to privacy in Nigeria, especially to avoid unnecessary conflation that comes with mixed approaches, which may hamper both academic and practical appreciation of the interests protected by the right-based approach as opposed to the expectation-based approach. The article has also traced the origins to the constitutional conferences of the late 1950s and the eventual affixing of the Bill of Rights to the 1954 Constitution as a political tool in anticipation of the general elections of 1959. The article emphasises the role played by the European Charter and its transplantation as the Nigerian Bills of Rights by concluding that, from a privacy perspective, European law represents a persuasive precedent for Nigeria.

African Journal on Privacy & Data Protection

To cite: EC Joseph & ME Mwakisiki 'Protection of children's rights to privacy in cyberspace: A bird's eye view over the Tanzanian legal framework ' (2025) 2
African Journal on Privacy & Data Protection 98-125
https://doi.org/10.29053/ajpdp.v2i1.0006

Protection of children's rights to privacy in cyberspace: A bird's eye view over the Tanzanian legal framework

*Elias C Joseph**
Assistant lecturer, Moshi Cooperative University; practising advocate, Kilimanjaro, Tanzania

*Mwakisiki E Mwakisiki***
Practising advocate, Kilimanjaro, Tanzania

Abstract

Children's privacy rights in cyberspace are essential aspects of today's digital age. This is because children's exposure to cyberspace is inevitable given its relevance in children's communication, education, recreation opportunities and cultural exchange. Moreover, these rights underpin other important rights, namely, dignity, public participation, information access, freedom of expression and right to associate. The right becomes more pressing given an increase in children's connectivity in cyberspace. This article focuses on unveiling the inevitable ever-growing landscape of child exposure to cyberspace in Tanzania and the current and potential privacy risks associated with their navigation in cyberspace. The article also explores the legal and policy challenges, implications and efforts to address these challenges. The study employs doctrinal analysis, archival research and case

* LLB (Mzumbe University) PGDLP (Law School of Tanzania) LLM (University of Iringa); josephbr945@gmail.com
** LLB (Moshi Cooperative University) PGDLP (Law School of Tanzania); mwakisiki.mwakisiki@mocu.ac.tz

study methodologies. Appropriate human rights instruments of international nature were studied to situate the discussion to a broader perspective. Additionally, secondary materials such as government reports, surveys, reports from non-state actors and newspapers were used. The approach ensures a thorough analysis of the complex socio-legal issues surrounding children's privacy in cyberspace. The study further employs a comparative analysis and benchmarking of the existing legal and policy framework against international best practices and standards. The purpose is to draw lessons from and to inform the suggested reforms in the law on minors' privacy in Tanzania. The article underscores that, for children to peacefully access and exploit opportunities brought by the virtual world, a comprehensive legal and policy framework tailored towards protecting children's rights in cyberspace becomes essential. Collective measures between actors are imperative in safeguarding children's privacy rights in cyberspace.

Key words: right to privacy; child privacy; cyberspace; Tanzanian legal framework

1 Introduction

The virtual world has become an integral part of every facet of human life, influencing the way in which people engage, connect and communicate.[1] In today's technologically astute society, children are increasingly immersed in the virtual world, making their involvement in the digital realm inevitable. Their engagement in the virtual world is seen as a necessary means for them to share and effectively engage in their civic life.[2] With over two billion children forming a significant portion of the global population,[3] more than 70 and 90 per cent of children had access to laptops and smartphones respectively.[4] This significant exposure to the virtual environment brings about both benefits and a spectrum of risks.[5] For instance, research indicates that more than 300 million children, experience online sexual exploitation and abuse yearly.[6] Therefore, while it is true that the virtual world offers numerous benefits to children's growth and development, it also renders them more vulnerable to privacy breaches and exploitation.[7]

1 According to art 1 of the Convention on the Rights of the Child, a child means every human being below the age of 18 years unless under the law applicable to the child; the majority is attained earlier.

2 I Milkaite & E Lievens 'Children's rights to privacy and data protection around the world: Challenges in the digital realm' (2019) 10 *European Journal of Law and Technology* 4.

3 Children in the World by Country 2024, https://worldpopulationreview.com/country-rankings/children-in-the-world-by-country (accessed 5 June 2024).

4 Share of children and adults worldwide using selected digital devices as of December 2023, https://www.statista.com/statistics/1483634/children-adult-devices-access-worldwide/ (accessed 13 December 2014)

5 M Cunha 'Child privacy in the age of web 2.0 and 3.0: Challenges and opportunities for policy' Innocenti Discussion Paper (2017) 6.

6 Scale of online harm to children revealed in global study, https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-global (accessed 13 December 2024).

7 UNICEF 'Children's online privacy and freedom of expression' Industry Tool Kit (2018) 4.

Fascinated by the virtual world and because of their immaturity, children may inadvertently share their data, putting themselves at risk of cyber-bullying and exposure to inappropriate content, among other dangers.[8] For these reasons, their security in online atmosphere has become an emerging topical and critical issue gaining prominence across jurisdictions.[9] Furthermore, the need to address children's privacy rights hinges on the reality that it is a fundamental right underpinning other essential rights including freedom of expression, information and association.[10] Thus, protecting children's privacy rights not only is an imperative human right but also a conditional precedent for building a stable and prosperous nation in the future.

As in the case of many African countries, Tanzania has fully embraced technological advancement, integrating it in different spheres of life, including children's education and development.[11] Over the past decade, Tanzania has experienced a demographic shift towards a youthful population, with approximately 43 per cent of its population comprising children below 15 years.[12] Although statistics on children's involvement in cyberspace in Tanzania are scant, the few available are worth mentioning. The 2022 report by ECPAT, INTERPOL and UNICEF shows that 67 per cent of minors of 12 to 17 years are internet users.[13] Such an ever-increasing number of children's population, coupled with their growing involvement in cyberspace, indicates the need for a critical examination of their rights while navigating these cyber platforms. This need is further underscored by the fact that children previously were not part of both international and domestic debates on technological regulation, which so far has resulted in the promulgation of regulations that do not specifically consider children's welfare.[14] Additionally, children are now at the centre of several global agendas such as the 2030 Global Agenda which, among others, aims at building a bright future and safer environment where children can harness their full potential and secure their rights.[15]

Appreciating the essence of protecting children's rights and upholding its international obligations, Tanzania has so far made significant strides in developing specific legal frameworks aiming at safeguarding children's rights. The enactment of the Child Act of 2009, the Cyber Crimes Act of 2015 and the

8 L Fourie 'Protecting children in the digital society' in J Grobbelaar & C Jones *Childhood vulnerabilities in South Africa: Some ethical perspectives* (2020) 232-234.
9 M Macenaite 'Protecting children's privacy online: A critical look to four European self-regulatory initiatives' (2016) 7 *European Journal of Law and Technology* 2.
10 Privacy International and Tanzania Human Rights Defenders Coalition *Stakeholder Report* (2015) 2.
11 K Okeleke '*Digital transformation in Tanzania: The role of mobile technology and impact on development goals*' (Groupe Speciale Mobile Association 2019) 19.
12 *'The 2022 Population and Housing Census: Age and Sex Distribution Report, Key Findings, Tanzania'* (2022) 9.
13 ECPAT, INTERPOL & UNICEF *Disrupting harm in Tanzania: Evidence on online child sexual exploitation and abuse* (Global Partnership to End Violence against Children 2022) 24.
14 Okeleke (n 11) 18.
15 Adopted by United Nations member states on 25 September 2023; all forms of child violence, abuse and exploitation were integrated as an international development agenda (para 16.2).

Personal Data Protection Act of 2022 supports this assertion.[16] Complementing these legislative initiatives, Tanzania recently launched the Child Online Protection (COP) campaign, which aims at safeguarding children in digital realms.[17] The Tanzania Communication Regulatory Authority, on its part, through the Computer Emergency Response Team (CERT), has regularly been issuing guidelines to parents and guardians on practices enhancing children's security while online.[18] Despite these efforts, more is still to be done, as the risks children face in the digital environment keep on increasing.[19] Against this backdrop, it thus is important to evaluate the Tanzanian legal framework, assessing the degree at which minor's privacy rights in the digital setting have been upheld and realised.

This article delves into the intricate landscape of the cyberspace by examining how some activities involving children have necessarily shifted their environment from physical to virtual environment. It unpacks the inevitability of cyberspace for children and the various risks and implications associated with their exposure to it. It explores the legal, institutional and other measures implemented to preserve children's privacy online both in Tanzania and globally. The article emphasises the importance of collaborative measures among relevant stakeholders, for instance, the government, regulators, technology companies, internet access providers, children, and parents or guardians, in an endeavour to create a safe online atmosphere for children.

The article is organised in six parts, starting with this introductory part, which provides a brief background and underscores the necessity of safeguarding children's privacy in cyberspace. The following part offers an elucidation of important concepts, namely, child protection, cyberspace and child privacy, while offering the divergent views between Afrocentric and Eurocentric schools on the conception of the term 'privacy'. The subsequent part provides an account of the trend of exposure of children in cyberspace and the prevalent violations of their privacy rights. The fourth part makes an evaluative analysis of existing legal frameworks at domestic, regional and international levels, and the ensuing part examines the position of the Tanzanian courts in vindicating children's privacy rights. The article concludes by encapsulating the main findings and recommendations derived from the preceding discourse.

16 *Stakeholder Report* (n 10) 4-7.
17 The campaign to protect children online launched on 19 February 2024, https://dailynews.co.tz/campaign-to-protect-children-online-launched/ (accessed 13 December 2024).
18 Protection of children online, https://www.tcra.go.tz/pages/child-online-protection-cop (accessed 13 December 2024).
19 Okeleke (n 11) 45.

2 The conceptions of 'child protection', 'cyberspace' and 'child privacy'

To develop a well-founded understanding of the gist of this work, it is significant to conceptualise the terms 'child protection', 'cyberspace' and 'child privacy' in the purview of this article. This is imperative because some concepts bear relative connotations depending on the scholarship taken as a standpoint, the societal characteristics, and the economic and cultural environment. Child protection entails safeguarding children against abuse, violence, neglect, exploitation together with implementing several efforts to respond to harm directed towards children.[20] The concept broadly includes protection in all settings, the cyber environment included.[21] Crucially, it encompasses all efforts for deterrence of and response to all types of children's ill-treatment.[22] Emphasising the protection of children's privacy, in *Centre for Child Law & Others v Media 24 Limited & Others*,[23] the South African Court held that centrality of children's privacy rights to their self-identity renders it even more crucial than for other demographic groups.

On the other hand, the term 'cyberspace', as defined in *Webster's new world telecom dictionary*,[24] refers to the virtual environment formed by interconnected computers and computer networks on the internet. It entails data, objects and activities that exist in the network itself.[25] Essentially, it represents the realm where computers and individuals engage, typically through the internet.[26] The term is synonymous with the term 'internet' and, therefore, anything happening on the internet is considered to take place within cyberspace rather than at the physical location of the servers or users.[27] Coming to the concept of 'child privacy', one of the difficulties facing effective protection of privacy rights is the rhetorical battle cry in a plethora of unrelated contexts of the notion of privacy.[28] Some claim that the notion encompasses a variety of interconnected yet distinct notions, including the right of being alone, controlled access to oneself, secrecy, power

20 AK Johnson & J Sloth-Nielsen 'Child protection, safeguarding and the role of the African Charter on the Rights and Welfare of the Child: Looking back and looking ahead' (2020) 20 *African Human Rights Law Journal* 644.
21 As above.
22 As above.
23 [2019] ZACC 46.
24 R Horak *Webster's new world telecom dictionary: A comprehensive reference for telecommunication technology* (2007).
25 Protecting Children in Cyberspace, https://mpra.ub.uni-muenchen.de/17150/ (accessed 5 June 2024).
26 SMH Collin *Dictionary of ICT* (2004).
27 Johnson & Sloth-Nielsen (n 20) 644.
28 *The right to privacy in the digital age in Africa: Module 1 – Introduction to privacy and data protection* Massive Open Online Course (MOOC) presented by the Centre for Human Rights, University of Pretoria, supported by Google, 27 May 2021.

over individual data, and personal hood.[29] However, a common thread among these diverse interpretations is the desire for control over personal information.[30]

Contextually, some African authors have been quick to point out that the African conception of the term 'privacy' relatively differs from the outside world. They assert that the prevailing understanding of privacy is Eurocentric and does not align with African realities.[31] Thus, to them, a proper definition of the term 'privacy' has to take on board the inherent features of communality, collectivism and interdependence existing in African societies.[32] Moreover, child privacy should be conceptualised taking on board the parental role of reasonable control over the behaviour of their children.[33] However, this school is still debatable given that, to date, there is no universally agreed upon definition of privacy in African social-political context.[34] Therefore, the notion of child privacy online can also be discussed in conjunction with the above viewpoint, because similar sentiments arise when discussing concepts relating to children's privacy in cyberspace. Child privacy in cyberspace consequently is associated with exposure to private data and various forms of harm, including solicitation of children for sexual purposes, exposure to inappropriate content, manipulation, surveillance, hacking and damage to reputation, among others.[35] According to the United Nations (UN), the phrase 'children's online privacy' encompasses all facets of child's privacy, including physical, communication, informational and decisional aspects.[36]

To this end, it is argued that the efforts by Afrocentric views to conceptualise privacy, taking on board the inherent characteristics in Africa, have not been realised. The article notes further that such a dilemma might have contributed to the information gap regarding the conception and essence of children's privacy online in African jurisdiction. In Tanzania, for instance, the Tanzania Communication Regulatory Authority (TCRA) issues quarterly statistical reports on the trend of accessibility and involvement of people in the internet. The report does not show the trend in terms of age and, therefore, one cannot comprehensively assess the growth of children's experience in the internet.[37] This situation is alarming given that any contemporary landscape on data protection should take on board the needs of the children. The World Health Organisation (WHO) emphasises that children's concerns need be at the core of

29 EC Joseph 'Right to privacy in mobile communication in Tanzania' (2022) 1 *Journal of Contemporary African Legal Studies* 48.
30 A Makulilo 'The quest for information privacy in Africa' (2018) Book Review Reply, *Journal of Information Policy* 317-337
31 As above.
32 Joseph (n 29) 48.
33 Art 10 African Charter on the Rights and Welfare of the Child, 1990.
34 J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 19.
35 OM Sibanda 'Towards a more effective and coordinated response by the African Union on children's privacy online in Africa' (2022) *African Human Rights Yearbook* 158.
36 UNICEF (n 7) 4.
37 Tanzania Communications Regulatory Authority, Quarterly Statistics Reports, https://www.tcra.go.tz/ (accessed 26 December 2024).

any Sustainable Development Goals (SDGs).[38] It was imperative, therefore, for TCRA reports to have a section showing the trend of children's accessibility to the internet to inform the government on the potential and magnitude of their risks while navigating there.

3 Children's exposure to the cyberspace

Lifestyle changes brought about by the advancement of information and communication technology have not left children behind. Today's children grow with the internet, to the extent of becoming digital natives.[39] The internet and other online conduits have attracted children in their endeavour to engage, communicate and learn.[40] Millions of children access the internet annually for educational and recreational purposes.[41] However, in their attempt to explore the opportunities available over the internet, such as playing, learning, self-expressing, experimenting relationships and identities, they find themselves unwittingly sharing an increasing amount of their personal data to service providers.[42]

The ever-increasing children's involvement in the digital realm stems from, among other things, concerted efforts to achieve digital inclusion and the essence of bridge the existing digital divide.[43] In 2020, for example, it was estimated that 87 per cent of children in advanced economies and 6 per cent in emerging economies had internet accessibility.[44] Additionally, according to the global telecommunication authority, 65 per cent of young persons in the developing world connect to the internet for various activities.[45] Irrespective of the digital divide in Africa, by 2021 about 40 per cent of young people were able to get the internet connection in any of its forms.[46] A survey conducted in Ghana on minors' engagement in the digital realm has shown that, on average, children begin using the internet at the age of 12 years, with four out of ten children accessing the

38 Children as a Basis for Sustainable Development, https://sustainabledevelopment.un.org/content/documents/6449100-Children%20as%20a%20basis%20for%20sustainable%20development.pdf (accessed 26 December 2024).

39 OECD 'The protection of children online: Risks faced by children online and policies to protect them' (2011) *OECD Digital Economy Papers* 179.

40 A Singh & T Power 'Understanding the privacy rights of the African child in the digital era' (2021) 21 *African Human Rights Law Journal* 100.

41 M Medaris & C Girouard 'Protection of children in the cyberspace: The ICAC task force programme' (2002) *Juvenile Justice Bulletin* 1.

42 M Macenaite & E Kosta 'Consent for processing children's data in the EU: Following in US footsteps?'(2017) 26 *Information and Communications Technology Law* 146.

43 See item 4 of the introduction to General Comment 25 on children's rights in relation to the digital environment.

44 UNICEF & International Telecommunication Union 'How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic' (UNICEF, New York, 2020) 4.

45 Joining Forces Alliances 'Protecting children in the digital environment' (2023), cited from the 2022 Safer Internet Day – We must act together to put children and young people at the centre of our digital policies.

46 A Singh & T Power 'Understanding the privacy rights of the African child in the digital era' (2021) 21 *African Human Rights Law Journal* 100.

internet at least once a week.[47] This indicates that children frequently utilise the internet and they do so at a relatively young age. In Africa, generally, the survey shows that out of an estimated 590 million internet users as of May 2022, one-third were children.[48]

In Tanzania, while there has not been an extensive and regular survey on the trend of children's involvement in cyberspace, a few available reports are worth noting. The available data shows that internet penetration stands at 37.6 per cent with a growth rate of 20.024 per cent. In August 2023, the internet users in the country reached 23 142 100.[49] Furthermore, the statistics indicate that as of June 2022, approximately 67 per cent of young persons above 12 and below 18 years in Tanzania were internet subscribers.[50] Alarmingly, 4 per cent of these children were reported to have experienced online sexual abuse.[51] The abuse typically involved blackmail and solicitation to participate in sexual related activities such as sharing explicit pictures.[52] While the 4 per cent may seem insignificant, it translates to roughly 200 000 children, which is a significant number.

The above statistics highlight the growing reliance on the use of the internet by children, making it an important factor that determines their learning and growth.[53] This makes the internet an important facet through which children's cultural exchange is effected.[54] Given this reliance, there is a pressing need for an inclusive and responsible use of the internet and its related technologies. However, this will require collaboration from the global community and the active participation of all stakeholders to guarantee the safe and secure navigation of children in online platforms globally.[55] It therefore goes without saying that effective child protection in cyberspace should take on board all-important stakeholders in their facets, such as children themselves, parents, educators, the online industry and policy makers, to mention but a few.[56]

47 'Risk and opportunities related to children's online practice' UNICEF *Ghana Country Report* (2017) 10-11.

48 Access to the digital environment for children: Building safer and inclusive digital spaces for refugee children with special needs and disability, https://reliefweb.int/report/world/access-digital-environment-children-building-safer-and-inclusive-digital-spaces-refugee-children-special-needs-and-disability (accessed 12 June 2024).

49 Internet Users Statistics for Africa, https://www.internetworldstats.com/ (accessed 12 June 2024).

50 Rising child abuse cases in Tanzania force review of law, https://www.theeastafrican.co.ke/tea/news/east-africa/tanzania-child-law-3912468/ (accessed 12 June 2024).

51 As above.

52 As above.

53 UNICEF (n 47) 10-11.

54 International Telecommunication Union (ITU) & UNICEF *Guideline for industry on child online protection* (2015).

55 International Cooperation on Child Online Protection, Expert Consultation on ICTs and Violence against Children in Costa Rica, 9-10 June 2014. International Cooperation Child Online Protection

56 Singh & Power (n 40) 100.

4 Protection of children's rights to privacy in cyberspace at global, regional and domestic legal levels

4.1 Protection of children's rights to privacy in the cyberspace at global level

Privacy as a right gets refuge from article 12 of the Universal Declaration of Human Rights (Universal Declaration) of 1948. The Declaration, among other things, discourages arbitrary interference in people's privacy.[57] In similar vein, the International Covenant on Civil and Political Rights (ICCPR) replicates article 12 of the Universal Declaration by obliging states to enact laws to uphold the right of its individuals' privacy.[58] It may be speculatively said that these articles referred to privacy in the traditional physical setting as opposed to the virtual world. This argument is supported by the idea that in 1948 and 1966, when the Declaration and ICCPR were enacted, the level of technology was such that the drafters could not be expected to contemplate the possibilities of what is currently evidenced. That might be the reason that moved the UN later on affirm that any right protected offline is equally protected online.[59]

Alongside the two instruments, there is the UN Convention on the Rights of the Child (CRC).[60] This Convention has received nearly universal acceptance and, arguably, is the most detailed convention in the field of child welfare. However, CRC suffers the same challenge as the Universal Declaration and ICCPR as it was promulgated when children's involvement in cyberspace was still in its infancy and, therefore, it lacked the current technological inputs necessary in upholding children's entitlements in cyberspace.

CRC through article 17 requires states to enable children with information access from different sources within and without the national boundaries, in order to promote their social, spiritual, mental and physical well-being.[61] Under paragraph 9 of General Comment 25 on children's rights in relation to the digital environment, state parties are obliged to create an environment for equal opportunity for children to connect with the online atmosphere and efforts are made to minimise digital exclusion. This includes free and safe access for the children to utilise for education, home and recreational settings.[62]

57 Art 12.
58 Art 17.
59 Resolution 3 of General Assembly Resolution 68/167 was adopted on 18 December 2013.
60 A*dopted by the UN General Assembly on 20 November 1989 and entered into force on 2 September 1990. Tanzania acceded to this Convention on* 1 June 1990.
61 Art 17(1) CRC.
62 CRC Committee General Comment 25 (2021) on children's rights in relation to the digital environment.

In similar vein, state parties to CRC and parents or guardians are obliged to ensure that proper guidelines exist, shielding them from destructive information.[63] It can therefore be argued that it is the spirit of CRC that children should be afforded tools for accessing information and materials across the globe. In the modern era, these tools may include computers, smartphones, tablets and the internet, to mention but a few. It therefore is against the spirit of CRC for governments not to put deliberate measures enabling children's accessibility to the cyberspace enjoying rights such as communication, education and recreation. Additionally, while these children are exercising their rights to exploit the potentials inherent in cyberspace, states in collaboration with guardians have to guarantee that they are free from any harm to their well-being in all facets.

Moreover, CRC in article 12 demands children to be accorded the right to be heard on any matter touching them, relying on the age and the adulthood of the child. Interpreting what 'matters affecting children' means, General Comment 25 states that it means all matters which children's perspectives can improve the quality of the solutions.[64] Arguably, these include enacting laws affecting children or regulating technologies having impacts on their lives.

However, whether or not a child's view should be considered depends on the power of making their opinions, appreciate and evaluate the consequences of the matter, and this has to be taken on after consideration of several factors,[65] given that parents or legal guardians reasonably maintain the control, over their behaviours.[66] This parental responsibility or supervisory right, however, needs to be exercised depending on the evolving capacity of the particular child.[67] Evolving capacity is a concept imported by CRC as a basis for assessing the understanding of the child of the risks in cyberspace independently of their parents or guardians. Parents and guardians are empowered to take charge of that.[68] It is a principle on child's gradual attainment of competencies, understanding as well as agency. CRC under this principle considers the age and development stage of a child as a yardstick for assessing a child's independent engagement from parents and guardians in the digital setting.[69] Therefore, efforts designed to uphold children's privacy rights in their endeavour to access cyberspace should consider the uneven position of children, their competence, understanding, and the associated nature of the risks.[70] Against the above backdrop, it thus is fair to state that it is a violation of CRC to enact laws regulating children's experience in cyberspace without allowing them to air their views on how they want it to be dealt with. Moreover, this is more so because privacy rights of a child are more pressing

63 Art 17(2) CRC.
64 CRC Committee (2009) General Comment 12: The right of the child to be heard para 27.
65 General Comment 12 (n 64) paras 28, 29 & 30.
66 Art 5 CRC.
67 As above.
68 General Comment 25 (2021) on children's rights in relation to the digital environment para 19.
69 As above.
70 As above.

than that of other groups, given the fact that the same are central to their self-identity.[71] State parties should ensure parents and guardians are aware and equally respect children's evolving capacities, autonomy and privacy. They should play a facilitative role in acquisition of digital literacy to children and realisation of their rights, including protection in the digital settings.[72]

Article 16 of CRC prohibits unlawful and arbitrary interference with a child's privacy, including that of his family, and correspondence, and it further requires legal protection against encroachment or attacks on the child's privacy. It has therefore been contended that a child's privacy is threatened by several activities, namely, unregulated data gathering and profiling done by multiplicity of stakeholders, and by the different actions by members of the family. The activities range from sharing photographs or information online by parents or guardians or strangers.[73]

4.2 Protection of children's rights to privacy in cyberspace in Africa

In the African context, upholding children's privacy rights is multi-regulated across several legal instruments, both specific and general, the main instrument being the African Charter on the Rights and Welfare of the Child, 1990 (African Children's Charter). The Children's Charter plays a notable role in safeguarding children's privacy rights in the region. The Charter expresses a child as an individual of less than 18 years of age.[74] Article 12 of the Charter, moreover, guarantees the right of minors to participate in sports and games suitable to their age.[75] This would cover both recreation available online and traditional offline recreations. Despite providing for learning platforms, recreation, social inclusion and civic participation to the young generation, the digital revolution has brought with it new forms of opportunities for harm to children.[76] Moreover, pandemics such as COVID-19 escalated online child abuse and exploitation.[77] These challenges call for a systemic approach as opposed to an issue-based approach.[78]

Under article 10 of the African Children's Charter, a child is protected from arbitrary or unlawful encroachment to their privacy in all its facets.[79] This provision extends to include protection of privacy rights in the cyberspace. This is because international standards require that similar rights that one enjoys

71 CCT261/18 [2019] ZACC 46; 2020 (3) BCLR 245 (CC); 2020 (1) SACR 469 (CC); 2020 (4) SA 319 (CC) (4 December 2019).
72 General Comment 25 (2021) on children's rights in relation to the digital environment para 21.
73 YE Ayalew, V Verdoodt & E Lievens 'General Comment No 25 on children's rights in the digital environment: Implications for children's right to privacy and data protection in Africa' (2024) 24 *Human Rights Law Review* 6.
74 Art 2.
75 Art 12(1).
76 Johnson & Sloth-Nielsen (n 20) 664.
77 As above.
78 Johnson & Sloth-Nielsen (n 20) 665-666.
79 Art 10.

offline should further be enjoyed online.[80] State parties are therefore expected to uphold and guarantee privacy rights in the context of digital communication.[81] Similarly, laws are expected to guarantee and protect privacy online as it does offline.[82] Paragraph 97 of General Comment 25 on children's rights in the digital environment[83] requires regulations relating to the digital environment to be compatible and to keep pace with principles in the offline atmosphere. This means that legislation should afford a similar level of protection to online rights as it does to rights that are enjoyed offline.

Moreover, the African Children's Charter stresses the best interests of the child as the paramount principle in any act performed in relation to children.[84] This principle is dynamic and context-specific and, in assessing it specifically in a digital environment, regard should be had to all children's rights. Under article 4(2) of the Charter, it is against that principle for the government to pass a decision affecting children without affording them a right to air their views directly or through their representatives. Equally, online commercial activities such as advertising and marketing accessible to or targeting children should pay due regard to the genuine opinion of the said children who possibly may be victims or beneficiaries of the activity.[85] Nonetheless, in assessing what amounts to the child's best interests, transparency is of the essence.[86] In the absence of transparency, practices such as profiling, behavioural targeting, information filtering, automated data processing, mandatory identity verification and mass surveillance arbitrary interfere with the child's identity, location, emotions, health, relationships and biometric information, among others.[87] Consequently, this may occasion an everlasting consequence on the child's agency, dignity, health and exercise of their rights.

The only justification for interference with the privacy of children in cyberspace is if same meets the minimum thresholds of being provided by the law, for legitimate purposes, proportionate and designed to observe the best interests of the child, for upholding data minimisation, and should not be inconsistent with the aims and objectives of international standards.[88] Practices such as surveillance and automated processing of children's data, if routinely conducted and if made without parent or guardian consent, are held to be inconsistent with international standards.[89] Therefore, practices such as monitoring of children done for lawful

80 Resolution 3 of General Assembly Resolution 68/167 was adopted on 18 December 2013.
81 Resolution 4 of General Assembly Resolution 68/167 was adopted on 18 December 2013.
82 Resolution (A/RES/71/199) on the right to privacy in the digital age, 2016.
83 CRC Committee General Comment 25 (2021) on children's rights in relation to the digital environment.
84 Art 4.
85 See para 41 of General Comment 25 (2021) on children's rights in relation to the digital environment.
86 See the principal of the best interests of the child.
87 See para 68 of General Comment 25 (2021) on children's rights in relation to the digital environment.
88 See para 69 of General Comment 25.
89 See para 75 of General Comment 25.

and necessary purposes such as safety should be carefully implemented so that it does not prevent a child from enjoying other rights such as access to a helpline and important information.[90] It is suggested that to reduce the risk, programmes hiding child identity while online, such as avatars or pseudonyms, should be employed. These programmes, however, should be carefully handled and should not turn and help in hiding harmful behaviours, especially those that may even come from unscrupulous parents or guardians.[91]

Another significant instrument in Africa is the African Union Convention on Cyber Security and Personal Data Protection, 2014 (Malabo Convention).[92] The Convention intended to guide legislative bodies of member states in enacting legislation on internet security, data protection, cybercrimes and online transactions.[93] The Malabo Convention has not been operative because it has not attained the ratification thresholds.[94] Moreover, Tanzania is yet to be a signatory to the Malabo Convention.[95] The Convention contains some valuable provisions about safeguarding children's abuse or exploitation along with other pertinent rights such as privacy. Article 8(1) obliges state parties to put in place a legal framework that protects data and punishes the violation of privacy rights. Further, article 29(1)(3) protects children against online exploitation by criminalising child pornography. Even though it does not directly address the question of violation of children's data and privacy, this Convention remains relevant in the field of data protection, inclusive of minors' information.[96] It underscores the importance of having an independent authority for preserving of personal information. It unpacks the six principles of data processing without which privacy of personal data cannot be attained. These include consent, lawfulness, fairness, purpose, relevance, storage, confidentiality, accuracy and security. Although it is not currently in force in Tanzania, it continues to serve as a valuable framework for developing robust policies, laws, and institutions that align with international standards on data privacy as a key component of privacy.[97] Nevertheless, sound protection calls for the Tanzanian government to accede to the Malabo Convention as it will be bound by its provisions upon its coming into operation.

90 See para 76 of General Comment 25.
91 See para 77 of General Comment 25.
92 Also known as the Malabo Convention, drafted in 2011, and adopted on 27 June 2014. The Convention has not yet entered into force because under art 36 the treaty will only enter into force after the 15th instrument of ratification or accession has been deposited, but only 5 countries have managed to deposit or accede to this Convention so far.
93 Joseph (n 29) 56.
94 See the List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 29 December 2024).
95 African Union Convention on Cyber Security and Personal Data Protection, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 20 December 2024).
96 A model law on data protection (SADC Model Law on Data Protection (2013)) which provides guidance on framing data protection legislation is available for member states.
97 Joseph (n 29) 55.

4.3 Protection of children's rights to privacy under domestic legislation

Tanzania is a signatory to several conventions guaranteeing children's rights and entitlements.[98] Consequently, several pieces of legislation have been enacted for a similar purpose.[99] However, while the adequate safeguard to children's privacy rights in cyberspace requires a robust technologically driven legal and policy regime, the existing policy and legal framework in Tanzania is challenged by the evolving nature of cyberspace. It is therefore argued that with the lack of such comprehensive legal and policy regime tailored towards protecting children's rights to privacy, the protection of children's privacy rights, especially in cyberspace, becomes a mystery.[100] The upcoming part will examine the child protection legal regime in Tanzania and its relevance in guaranteeing children's privacy rights.

4.3.1 Constitution of the United Republic of Tanzania

This is the *grundnorm* establishing the validity of other enactments. The Constitution asserts that any legislation in conflict with it is void to the extent of such contradiction.[101] It may be argued that before the inclusion of the Bill of Rights in the Constitution in 1984,[102] the right to privacy was not explicitly guaranteed, with its protection left to be addressed in other laws such as criminal and property laws.

Among the human right conferred and protected by the Constitution is the privacy rights, in general, and specifically the privacy of communication. Article 16(1) of the Constitution recognises privacy as a right and guarantees various aspects of it, including the privacy of private communication. However, this right is never absolute. Under article 16(2) the right to privacy may be limited under certain circumstances, but with specific reasons and procedures to be established by the law. Notably, the Constitution mandates that any limit to privacy rights must not violate the provisions that guarantee this right. The question of whether the requirements set forth under article 16(2) have been complied with by legislation limiting this right in Tanzania can be answered by an evaluation of each law limiting the right, an exercise falling in the purview of this part.

The right to privacy is further limited by a general clause in article 30(2) of the Constitution. This part prescribes that it is not unlawful to restrain the exercise

98 These include the Convention on the Rights of the Child,1989 and African Charter on the Rights and Welfare of the Child,1990.

99 For example, the Personal Data Protection Act of 2022; the Cybercrimes Act of 2015; the Electronic and Postal Communication Act of 2010.

100 SO Masocha 'Protection of children's rights to privacy and freedom from online exploitation and abuse in Southern Africa. A case study of South Africa and Zimbabwe' Master's dissertation, Makerere University, 2020 4.

101 Art 64(5) Constitution of the United Republic of Tanzania, 1977.

102 See the Fifth Amendment (came into operation in March 1985).

of a right, including the right to privacy, due to purposes such as protecting freedoms and the rights of others, public benefits, morality, defence, peace, safety and health. Essentially, this connotes that privacy rights can be curtailed for these reasons. In the case of *Kukutia Ole Pumpun & Another v The Attorney General & Another*[103] the High Court in interpreting this provision stated that a law restraining any individual right gets refuge under article 30(2) in the event the same meets the thresholds of being lawful in a manner that is not arbitrary. Furthermore, the law should incorporate suitable controls from arbitrary powers and offer an oversight to avoid misuse by those enforcing the law. Lastly, there should not be more restraints than what is essential to accomplish a lawful purpose.

Contextually, the Court's interpretation highlights that, while article 30(2) permits some restraints on the right to privacy, such limitations must meet the three-tiered threshold of legality, proportionality and legitimacy. If a law fails to meet these criteria, it violates article 16 of the Constitution. This implies that article 16(2), which allows laws to limit privacy without violating the Constitution, requires these laws to satisfy the three tests. This decision was further quoted with approval in the case of *AG v Dickson Paul Sanga*,[104] where a provision of a criminal procedural law denying bail to some bailable offences was saved by article 30(2) because it satisfied the proportionality, legitimacy and lawfulness tests. The Court in this case saved section 148(5) of the Criminal Procedure Act because the limit of the right to bail in the purview of this provision passes the above three-tier test. The restraint, therefore, was legal, proportionate and legitimate.

Furthermore, the Constitution under article 18(c) offers personal liberty to communicate and protection from interference in such communication. Unlike article 16(2), this provision contains no claw-back clause, indicating that the liberty to communicate without interference is not subject to legislative restraints. This appears to conflict with the wording of article 16(2), which permits the communication interference for some specific motives. However, article 30(2) seems to resolve this contradiction.

Additionally, the Constitution under article 30(3) allows anyone whose constitutional rights, including privacy rights, are violated or are likely to be violated, to file a suit in the High Court for redress. This provision offers legal recourse for anyone who believes that their privacy rights have been infringed upon. In remedying the infringement, the High Court may order the government to rectify the situation, amend the impugned provision or declare the provision or Act void.[105] However, this provision does not offer pecuniary redress to

103 [1993] TLR 159.
104 Civil Appeal 175 of 2020 (CA).
105 Art 30(5).

the victim, likely leaving this aspect to statutory legislation.[106] Moreover, this provision cannot be exercised if there is another law providing for redress.[107] This would literally mean that because certain laws criminalise acts related to privacy violations, such as interception of communication, this amounts to a redress to bar application of article 30(3). However, criminal liabilities do not always vindicate the victim of the violation. This is probably why article 16 of the Constitution requires the state to enact a law on how privacy can be regulated.

Therefore, the Tanzanian Constitution guarantees privacy rights. As the supreme law, it offers a framework through which laws restraining privacy rights should be premised. These premises to a large extent revolve around minimum safeguards set forth by international instruments such as ICCPR, such as legality, necessity, legitimacy and proportionality.[108] Therefore, it falls upon the statutes allowing limitation of privacy to consider these in their text.

4.3.2 Child Act, 2009

Enacted in 2009, the Child Act is a vital legislation in preserving children's rights in Tanzania. The Act promotes the well-being of children by incorporating the available international and regional standards on children's rights.[109] This Act fosters the welfare of the children by recognising the principle of the best interests of a child under section 4(2), laying the ground for safeguarding minors' privacy rights. In ensuring that personal information relating to children iskept secure, the Act contains provisions that guarantee confidentiality in child care and protection.[110] Despite the inclusion of several rights to be enjoyed by children in the second part of the Act, the right to privacy is not specifically stated. Furthermore, sections 9(3)(a) to (c) of the Act impose several duties and responsibilities on parents, such as protecting children from risks such as abuse, violence, neglect, exposure to physical and moral hazards, discrimination and oppression, but does not extend such duties to protecting children's privacy, particularly in the digital environment.

One of the peculiar features of this Act is the establishment of juvenile courts with the power to hear charges against children and handle children's care applications and maintenance matters.[111] The proceedings before the courts are conducted in a way that upholds the dignity and privacy of the concerned

106 See art 30(4).
107 Sec 8 Basic Rights and Duties Enforcement Act 33 of 1994.
108 UN Human Rights Committee (HRC) CCPR General Comment 16: Article 17 (Right to privacy), The right to respect of privacy, family, home and correspondence, and protection of honour and reputation, 8 April 1988, https://www.refworld.org/legal/general/hrc/1988/en/27539 (accessed 20 December 2024).
109 See the long title.
110 See part II-V.
111 Sec 97.

child.[112] While these courts provide an avenue to address cases where children are suspected of having committed offences, they do not have jurisdiction over violations of children's privacy rights, as their focus primarily is on cases where children themselves have allegedly violated the law.[113] This jurisdictional limitation restricts the scope of legal protection for children's privacy outside criminal or legal conflicts. In summary, while the Act provides a general legal regime for preserving children's rights, it does not explicitly guarantee minors' privacy rights, especially in the online ecosystem. The complementing laws that were expected to cover this void are also lacking. Therefore, this calls for an amendment of the Act to incorporate explicit provisions that guarantee children's privacy rights and extend the jurisdiction of juvenile courts to cover privacy violations.

4.3.3 Personal Data Protection Act, 2022

The Personal Data Protection Act, 2022 (PDPA) was brought in 2022 and came into operation on 1 May 2023. Through its long title, PDPA aims to provide principles for personal data protection, thresholds for the collection and personal data processing, establish an authority to oversee protection of personal information, improve the safety mechanisms for personal information controlled by a multiplicity of stakeholders and offer other related issues. It further aims at preserving the privacy of individuals in its different facets. In so doing, it regulates the gathering and handling of personal data, establishes a structural mechanism to safeguard personal information, protects data subjects and provides remedies thereto.[114]

Section 65 of PDPA gives freedom to data controllers to have in place ethical policies that describe ethics and conduct to be adhered to when collecting or processing personal data. However, the authority established has the power to approve the code of ethics before being operational. With this in mind, the law just sets the objectives and lets the service providers formulate procedures on how to achieve the objectives. The court has commended the practice for taking on board the neutrality of the privacy and data protection sector which cuts across several fields and, therefore, no possibility of a one-fit-all procedure.[115]

Section 23 authorises the collection of data by registered data controllers upon notification to the data subjects of the purposes, recipient, and if the purposes are authorised by the law.[116] This condition may be disregarded in a situation where such data is publicly available or if the data owner authorised collection from a

112 The practice and procedures before the juvenile court are governed by the Law of the Child (Juvenile Court Procedure) Rules, GN 182 of 2016.
113 Sec 98 of the Child Act (Cap 13 RE 2019).
114 Sec 4. The Act came into force on 1 May 2023 and it is complemented by Data Protection (Personal Data Collection and Processing) Regulations, GN 449C of 2023, published on 4 July 2023.
115 *Tito Magoti v Hon Attorney General* (Miscellaneous Civil Cause 18 of 2023) High Court Main Registry at Dar es Salaam.
116 Sec 23(2).

third party. This also applies if giving notice is impracticable, if non-compliance is necessary to comply with other written laws or if giving notice will affect the ground for their collection.[117] These wordings connote that this law authorises the gathering, use and unveiling of one's individual information without procuring permission from the information owner in the circumstances hitherto prescribed. These exceptions may be used as a loophole for violations of privacy specifically in the event the subject is a child. For instance, in a situation where a child's data has been unlawfully published, waiving the duty to seek consent from parents to process them would mean encouraging the unlawful publishing of a child's data. The other risk is in a situation where other written laws allow. The risk comes from the fact that PDPA is the only detailed legislation on safeguarding individual's data in Tanzania. It contains nearly all principles, limitations and minimum thresholds for the safe gathering and handling of personal data. Allowing personal data to be gathered under other laws whose enactments were not meant for security of data puts the right to data security in danger. This opens the doors for actors to opt for other laws whose requirements are not strict and overlook PDPA. The provision would have been protective if it stipulated that such laws must have incorporated similar or higher standard safeguards than PDPA itself. In line with this, in *Tito Magoti v Hon Attorney General*[118] the impracticable circumstances of waiving the requirement to obtain consent were supposed to be listed even if in general terms. The Court held the same about section 23(3)(e) which allows non-compliance with the requirement of consent if doing so would prejudice the lawful purpose of the collection. The lawful purpose ought to be defined to avoid abuse of the provision.

However, the Court ruled section 23(3)(d), which allows non-compliance where it is essential in adherence to other written laws, to be unproblematic. The Court grounded its argument on the fact that since laws are many and change over time, it is difficult to list all of them in a single Act. Much as one may agree with the Court on the fact that it is impossible to list all exceptions, it was prudent for legislators to qualify the statement that such other laws must adhere to the necessary minimum safeguards under PDPA. A blind relief to other laws to allow non-compliance may risk the privacy of personal data because the said other laws do not contain the minimum safeguards as it is in PDPA.

Section 30 imports the conception of sensitive data where the provision disallows any handling of sensitive personal information unless the subject consents in writing.[119] The Act under section 3 defines sensitive personal information to include data relating to children. The child's consent for data processing should be sought from the parents, guardian, attorneys, heirs or any other person recognised by law as such.[120] However, the requirement of consent

117 Sec 23(3).
118 As above.
119 Sec 30(1).
120 Sec 3.

is waived for several factors such as the requirement of other written laws, for purposes of protecting the child's important right or a third party, if it is essential for a legal claim, if the data is disclosed by the owner, for medical reasons or the interests of the child. Unfortunately, the Act does not define what vital interests of the child are to waive the requirement. In the absence of such meaning, this exception can be abused to the detriment of the child.

Notably, the Act is not explicitly clear on how the written consent envisaged by section 30 should be obtained especially in an online environment. In the USA, for instance, there is a federal law enacted to regulate children's privacy rights, that is, the Children's Online Privacy Protection Act (COPPA).[121] Crucially, COPPA presents the best practice on how consent should be sought and obtained. The Act requires website owners to display downloadable consent forms and parents to authenticate their age and identity.[122]

Moreover, some reasons warranting the revealing of personal data relating to a minor without a genuine authorisation of the parent or guardian are obsolete. For example, provisions such as section 30(5)(d)[123] allow the dealing with minors' data with no consent, merely because the minor himself or herself made the data public. Taking into account the fact that, generally, minors are not in a position to make rational judgments due to immaturity, this exception is unreasonable. The provision should have categorically stipulated that this provision relates to minors who in relation to their evolving capacities can form an independent judgment. This is different in other jurisdictions. For example, in Kenya, the only exception for the data controller to process the child's related data without a parent's or guardian's consent is if it is exclusively for providing counselling or services related to child protection.[124] In South Africa, dealing with individual's information about a child without the consent of a responsible person is if it adheres to an obligation in law. The rest must secure consent or at least sufficient guarantee is provided to ensure non-infringement of the child's privacy.[125]

Likewise, if the intention was that an obligation to notify be waived when the child's data is public owing to their parent's or guardian's act, the same is perplexing as it will mean subjecting a child to a violation of their privacy at the expense of their parent's or guardian's conduct. The situation becomes worse because the law does not require the permission of a parent or guardian to be genuine in terms of being free and informed.[126] This creates chances for ignorant and unscrupulous parents or guardians to consent to the detriment of the child's welfare.

121 Enacted in 1998 and it became operational in 2000. It has been amended from time to time to accommodate technological advancement and the online landscape.
122 See sec 312(5)(b)(i) of the Children's Online Privacy Protection Rule, 1999.
123 See sec 30(5)(d) of the Personal Data Protection Act, 2022.
124 Sec 33(4) of the Data Protection Act 24 of 2019.
125 Sec 35 of the Protection of Personal Information Act 4 of 2013.
126 Sec 2 of the Kenyan Personal Data Protection Act, 2019 defines consent to be the 'manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes'.

The Act remains quiet on its precedence in the event of provisions of other written laws being inconsistent with it in so far as the treatment of individual's data is concerned. The oversight creates room for laws with no minimum safeguards to apply to the detriment of children's rights. At the same time, the Act limits applications of its provisions where other written laws provide for another procedure. For example, section 33(2) relieves the data controller of a burden to communicate to the owner in case the same is under investigation according to other laws. Moreover, section 34(5)(a) is to the effect that the requirement of permission before processing data relating to a minor is immaterial in the event that other written laws provide otherwise.[127] Being a specific Act regulating personal data, it was supposed to take precedence over other written laws in the event of any inconsistency with respect to personal data. This is due to the fact that the Act incorporates necessary safeguards against violations of privacy while processing personal data lawfully when compared to other sector-specific laws.

Nevertheless, the Act bluntly exempts dealing with individual's data contrary to its provisions in any of the following circumstances:[128] if processing is made by the data subject himself for his personal use; if other laws or court orders require; if processing is made to safeguard national safety and security and public interest; if it is made for preventing or detecting crimes; if it is meant to detect or prevent tax evasion; if processing aims at investigating allegations of misuse of public funds and for reasons of vetting for nomination to a position in public service. The provision lacks checks against abuse of the loopholes. The provision should have provided minimum safeguards to any person utilising these exceptions. This has been the practice in international instruments and practices in other states such as Kenya, Uganda and Rwanda.[129]

Section 3 of PDPA defines a 'child' in accordance with the Child Act. Section 4(1) of the Law of the Child Act[130] describes a child as a human below 18 years. Therefore, literally under PDPA, all persons below the age of 18 require parental consent before accessing online platforms for any purpose whatsoever. The question is whether it is reasonable to subject the consent of all children to the consent of a guardian or parent. One may think of a child of 15 to 17 years curtailed with the right of access to online platforms unless their parent formally consents. Some jurisdictions have categorised these children as capable of consenting on their own, subject to the fulfilment of some preconditions.[131] The literatures

127 As an exception to sec 34(1), which requires consent before processing of personal data relating to a child, provides that '[s]ubsection (1) shall not apply where (a) the processing is necessary for compliance with other written laws'.

128 Sec 58(2).

129 See the Data Protection Act 24 Of 2019, Data Protection and Privacy Act, 2019 and Law Relating to the Protection of Personal Data and Privacy Law 58 of 2021.

130 Cap 13 RR 2019.

131 In Spain, eg, the data protection law contains specific provisions on the consent for the processing of data on minors. According to art 13 of the Spanish Personal Data Protection Law, 'data about data subjects over 14 years of age may be processed with their consent, except in cases when the law requires the assistance of parents or guardians'.

demonstrate that in most jurisdictions, the law determines the appropriate age boundary for a minor to consent.[132] This may be the reason why international instruments such as CRC imported the conception of evolving capacities in assessing the power of a child in accessing online platforms independent of their parent or guardian. It can therefore be rightly stated that relying on the general age of majority of the child may be unreasonable and impractical in some situations and environments. It was therefore reasonable, if the evolving capacities of a child was to be employed as a yardstick.

Another pertinent issue relates to the duty of the controller of data to have in place verification processes that guarantee determination of the age of minors and the genuineness of the permission. Age verification is central if the law targets the online services offered straight to children and more so to online services targeting the general audience or mixed audience.[133] This is paramount because surveys show that even the prevailing online service providers that specifically exclude children, such as Facebook, YouTube and Google, minors have been active users while treated as adults in these platforms.[134] In some jurisdictions such as that of Kenya, the law imposes a mandatory condition on the data controller to integrate a suitable mechanism for verifying the age and genuineness of the consent.[135] The contemplated systems are to be determined based upon, among others, the existing technology, the size of information processed, and the likelihood of risk to a child as a result of the processing of their individual information.[136] The highlighted standards are vital in curbing potential abuse of consent by parents, guardians or attorneys. This requirement is not captured in PDPA.

To wind up, PDPA was intended to be a general privacy and individual data safeguard law and it was expected to take precedence over other laws in case of inconsistency. This is because the other laws were not originally enacted to protect privacy or personal data. Therefore, PDPA vaguely warranting disclosure or collection of personal data under such other laws that do not contain the minimum safeguard, makes its enactment futile. The fact that PDPA contains minimum safeguards and preconditions before the disclosure or gathering of individual data, it ought to limit the exercise of other laws to the extent of the minimum standards enshrined therein. Moreover, PDPA should consider incorporating pertinent issues such as evolving capacity and age verification procedure requirements while avoiding blind and obsolete limits to the requirement of the law.

132 M Macenaite & E Kosta 'Consent for processing children's personal data in the EU: Following in US footsteps?' (2017) *Information and Communications Technology Law* 154.
133 Macenaite & Kosta (n 132) 173-174.
134 As above.
135 Sec 33(2) Personal Data Protection Act, 2019.
136 Secs 33(3)(a)-(e) Personal Data Protection Act, 2019.

4.3.4 Cybercrimes Act, 2015

The Act was brought in to establish and regulate crimes associated with the computer system, and information and communications technology. It aimed at providing the procedures to investigate, collect and use electronic evidence and related matters.[137] The cyberspace being central to this article makes the Act relevant. The Act makes crimes of some computer-related acts as having a bearing on personal privacy. It further regulates the accessibility of personal information needed for various purposes such as investigation of crimes. The Act describes a child for the sake of cybercrimes as an individual below 18 years of age.[138]

It moreover criminalises communication, disclosure or transmission of computer data to unauthorised persons. Equally, the law makes it unlawful for one to intentionally receive unauthorised computer data.[139] The offence is punishable with a fine. Alternatively, one may be imprisoned for one year or both. The Act creates an offence of data espionage. This relates to obtaining any computer data that is subject to protection against access without permission.[140] The contravention of this provision is punishable by a fine. The convict may alternatively serve a sentence of incarceration or both incarceration and fine. The offences do not make a distinction between the general data from some sensitive data such as that of children once unlawfully interfered with or unlawfully obtained.

The Act makes it unlawful to publish through computer systems or facilitate access to child pornography through computer systems.[141] This is an interesting move by the Act as it sets apart child pornography from those involving adults. The offence bears a punishment of not less than a fine of 50 million shillings or thrice the value of unjust benefits received by the convict. Incarceration of seven years and above or both fine and incarceration and a fine may be imposed. The provision displays the seriousness in addressing the problem by imposing a heavier punishment than it imposes on pornography involving adults.[142]

4.3.5 Electronic and Postal Communication Act, 2010

The Electronic and Postal Communication Act (EPOCA) is the main enactment in electronic communication whose intention, among others, was to keep abreast with developments in the electronic communications industry.[143] One

137 See the long tile to the Cybercrimes Act 14 of 2015.
138 Sec 3.
139 Sec 7(2).
140 Sec 8.
141 As above.
142 See punishment for the offence of pornography under sec 14.
143 See the long title of the Electronic and Postal Communication Act 3 of 2010. The Act came into force on 7 May 2010 and it repealed and replaced the Broadcasting Services Act, 1993.

of its objectives was to address challenges brought about by new technology.[144] First, the law obliges owners of a mobile SIM card to register it with the service provider[145] by submitting the subscriber's personal information.[146] It is believed that with such information the holders can monitor the communications of respective subscribers.[147] Section 98 obliges the service providers to maintain confidentiality of whatever personal information they acquire from subscribers.[148] This obligation is not reflected in the Tanzania Communications Regulatory Authority (TCRA) despite them having the power to retain a subscriber's information from service providers.[149]

Section 120 criminalises all conduct associated with communication interception such as interception, attempted interception or procuring another to encroach electronic communications,[150] disclosure or attempt to disclose information obtained by interception[151] and the use of the information obtained through interception.[152] However, nowhere does the Act attempt to vindicate the victim. EPOCA authorises the interception of communication and provides the duty of confidentiality to service providers' agents. The Act makes offences related to privacy such as any disclosure of intercepted communication by authorised persons.

Moreover, it limits service providers from accessing the communication for quality control purposes. Nevertheless, the law excludes TCRA from exercising confidentiality, something that puts the privacy of subscribers in jeopardy. It can, therefore, be argued that despite authorising interception of communication under other laws, it does not put in place adequate safeguards for privacy rights. Therefore, by doing so, it encourages unlawful interception by criminal investigators. Furthermore, this law fails to enlist the procedural mechanisms on how authorised individual may encroach such communication. This contravenes the constitutional provision of article 16(2) and that of article 17 of ICCPR which necessitates any law restraining privacy rights detail processes such as ways to challenge any misuse of such restriction and the redress possibility. ICCPR requires that in the event a communication is to be encroached, neutral authority should exist to authorise, and there must exist processes describing the environments, degree, and ways in which the work may be carried out and the remedy in the event the procedures have not been adhered ro by the responsible persons. The principles put forth by this Act do not give due regard to children and, therefore, protection enshrined therein is general.

144 Makulilo (n 30).
145 Sec 93(1) of the Electronic and Postal Communication Act 3 of 2010 and Regulation 4(1)(a) of the SIM Card Registration Regulations GN 112 of 2020.
146 Sec 93(2).
147 Makulilo (n 30) 4.
148 Sec 98(1).
149 Sec 91.
150 Sec120(a) of the Electronic and Postal Communication Act 3 of 2010.
151 Sec 120(b).
152 Sec 120(c).

4.3.6 Media Services Act, 2016

The Act was meant to provide promotion for professionalism in the media industry, to establish a board of accreditation for journalists, independent media council, and regime for regulating media services and other related matters.[153] Section 7(3)(f) of the Act obliges all media houses, while executing their responsibilities, to ensure that information aired out does not, among other things, involve unwarranted encroachment of an individual's privacy. Section 7(4) provides that the sub-part in this Act that regulates ownership, rights and obligations of media houses supersedes any provisions under any other written law in the event of inconsistency. This obligation concerns all online platforms.[154]

An analysis of the domestic legal framework has shown that, currently, several loopholes can be used by perpetrators to violate children's rights to privacy. As hitherto shown, some Acts provide general protection of privacy rights without giving due regard to the sensitivity of minors' privacy rights, while others provide obsolete or blind exceptions that may be abused against the interests of children's privacy rights. Others do not incorporate important issues such as the evolving capacities and age verification requirements. However, the highlighted shortfalls are not at all surprising. This is because legislation in middle and low-income countries has often trailed important technological advancement.[155] In that regard, the problem of legislating in the digital environment is well noted.

5 Role of the court in the protection of children's rights to privacy

The Constitution of the United Republic of Tanzania entrusts the judiciary of Tanzania with all judicial powers.[156] It is the judiciary that has the final powers in the dispensation of justice in Tanzania.[157] Therefore, when children's rights are violated, they have the right to seek appropriate remedies through established legal channels.[158] Principle 5 of the General Principles on Children's Online Privacy and Freedom of Expression acknowledges the complexity of achieving effective remedies, especially in a digital environment. It acknowledges that the availability of effective remedies depends on, first, a robust system of redress that ensures smooth resolution of complaints filed by children and their guardians; second, a transparent reporting mechanism that aligns with their digital literacy levels; and, third, the existence of avenues for further review or redress. However,

153 See the long title of the Media Services Act, 2016.
154 See the definition of media house, media services and media under sec 3.
155 M Hightower 'The Fourth Amendment and the dark web: How to embrace a digital jurisprudence that protects individual liberties (2021) *Georgetown Law Journal Online* 179.
156 See art 4(2).
157 See art 107B (1) of the Constitution of the United Republic of Tanzania,1977 as amended from time to time.
158 See CRC Committee General Comment 5 and Human Rights Committee General Comment 5.

the realisation of these rights is contingent upon the existence of a robust legal framework designed to preserve minors' rights. In the absence of a comprehensive and technologically driven legal framework tailored towards protecting children's privacy rights in Tanzania, this responsibility becomes the exclusive province of the courts. This vital role stems from articles 107A and 107B of the Constitution, which recognise courts as the guardians of citizens' rights.

In embracing their constitutional roles and mandates, Tanzanian courts have been instrumental in vindicating children's rights, especially those involving sexual violence and exploitation. Such cases have garnered significant court attention. The case of *Job Mlama & 2 Others v R*[159] serves as an example. In this case the appellants were charged with sexual exploitation contrary to section 138B(1)(e) of the Penal Code. It was alleged that the appellants jointly and together used violence to procure the child aged 13 years for sexual intercourse with a dog. In upholding its role in protecting children's rights and by acknowledging the victim's vulnerability as a child, the Court found the appellant's action inhumane and a serious violation of human rights.

In certain limited circumstances, the courts have also demonstrated sensitivity to children's rights by prioritising the right to privacy and the best interests of a child. In the case of *Kuruthum Omary Kahiba & Another v Mwajuma Omary Kahiba*[160] the Court considered privacy concerns when a minor sues for paternity. It was stated that, in such cases, the Court must prioritise the right to privacy and the best interests of a child. Additionally, in all criminal proceedings involving children, Tanzanian courts have consistently been showing respect for children's privacy while remaining mindful of their mandate and role in child protection. For example, in the case of *Sadick Hamad Ndiunze v The Republic*,[161] having noted that the victim was under the age of majority, the Court proposed to hide her actual name throughout the judgment for good reasons of preserving her respective integrity and privacy rights. It is worth commenting that this practice has consistently been applied by Tanzanian courts in all cases involving children.[162]

However, despite these notable developments, courts in Tanzania have not obtained enough avenues to vindicate children's rights to privacy outside criminal cases that relate mostly to child exploitation and abuse. This is because courts do not proactively seek matters to adjudicate unless parties are before it. Consequently, our courts have not yet tried a case where purely the violation of a child's privacy is at issue. This may be attributed to a low level of awareness of citizens' rights to privacy, which leads to a failure to understand the implications

159 Criminal Appeal 222 of 2012 [2013] TZCA 333 (30 July 2013) (unreported).
160 Misc Civil Cause 4 of 2018) [2020] TZHC 3597 (29 September 2020) (unreported).
161 Criminal Appeal 35 of 2022 [2023] TZHC 20683 (14 August 2023) (unreported).
162 See, eg, the case of *Kaimu Said v Republic* Criminal Appeal 391 of 2019 [2021] TZCA 273 (7 June 2021) and *Francis Petro v Republic* Criminal Appeal 534 of 2016 [2019] TZCA 304 (27 August 2019).

it has on the victim's well-being.[163] Moreover, the constitutional petitions filed in the High Court challenging provisions violating the right to privacy, generally, have often been unsuccessful on either technical or constitutional grounds.[164]

Several factors may be cited as the obstacles preventing the courts from fulfilling their role and mandate. First, unlike in disputes pertaining to children's mistreatment, there exists limited referral of cases to courts involving violations of children's rights to privacy. This limitation stems from ignorance of both children and parents about this important right.[165] Additionally, there is a lack of effective means for reporting and channelling children's claims, partly due to the existence of reporting systems such as Child Online Protection (COP) that do not adequately cover children's privacy issues and offer prompt responses to complaints filed by children. Second, since violations of children's privacy rights touch upon constitutional rights, they must be addressed by the High Court through constitutional petitions. The complex procedures involved in filing constitutional petitions in Tanzania deter children and their guardians from seeking redress.[166] For these reasons, the court's role in developing minors' rights jurisprudence is counselled.

On the contrary, other jurisdictions such as the Kenyan experience offer a good example of the role the courts can play in advancing children's rights to privacy in the online setting. The courts have so far been taking a progressive stance in affirming such rights by laying down legal principles that contribute to the advancement of children's rights jurisprudence. This is evident in numerous court decisions where children's rights to privacy were vindicated. A recent Kenyan case of *CMM & 6 Others v Standard Group & 4 Others*[167] suffices to illustrate the active part played by the Kenyan Supreme Court in protecting children's privacy rights. In this case, seven children were charged with arson. When the matter was called for hearing, the respondents, through their media outlets and platforms, publicly aired and published images and names of the children. The central issue was whether the alleged published images and names of children facing criminal charges, violated the children's privacy rights and that the acts by the respondents were not in the minors' best interest. In its considered judgment the Court decided that the acts by the respondent were violative of the appellants' privacy rights and the right for their best interests to be considered, as guaranteed under articles 31(c) and 53(2) of the Kenyan Constitution, respectively.

163 CIPESA 'Privacy and personal data protection in Tanzania: Challenges and trends' (2018) *State of Internet Freedom in Africa* 13, https://cipesa.org/download/reports/State-of-Internet-Freedom-in-Tanzania-2018.pdf (accessed 26 December 2024).

164 Eg, the case of *Magoti* (n 115).

165 S Shannon 'Protecting children's right to privacy in the digital age: Parents as trustees of children's rights' (2020) 36 *Children's Legal Rights Journal* 174.

166 See the Basic Rights and Duties Enforcement Act (Cap 3 RE 2019) and Basic Rights and Duties Enforcement (Practice and Procedure) Rules, 2014.

167 *CMM (suing as next friends of and on behalf of CWM) & 6 Others v Standard Group & 4 Others* Petition 13 (E015) of 2022 [2023] KESC 68 (KLR) (8 September 2023) (Judgment).

The Kenyan courts have also affirmed children privacy rights, stressing the importance of procuring consent before using children's images. In the case of *NWR & Another v Green Sports Africa Ltd & 4 Others*[168] the petitioner filed the petition against the respondents for violation of her children's rights to privacy after the respondents had taken and published the children's photographs without consent. Having found that the consent of the minor's parents or guardians was neither sought nor obtained, the Court ruled the act to be unlawful and a violation of the petitioner's constitutional rights.

The experience of Kenyan courts, therefore, highlights three crucial roles that the court can play in preserving children's privacy rights in the virtual setting. First, the court can define the boundaries of the constitutional right to privacy. Second, through bold pronouncements, it can establish a framework for addressing privacy complaints and developing jurisprudence to efficiently address infringement of children's privacy rights. Third, the courts can address current disparities in the legal framework, thereby shaping the landscape of children's rights jurisprudence.[169] Tanzanian courts, therefore, are urged to embrace these roles to fill the current gaps in the legal framework, a step that will be vital in moulding the legal landscape for children's rights in Tanzania.

6 Conclusion

This study has shown that children's privacy rights, especially in the virtual settings in Tanzania, are a critical issue that requires concerted efforts for their protection. The traditional legal framework in Tanzania has been challenged by the evolving nature of cyberspace, making children's privacy rights protection a nightmare. This calls for more robust and technologically driven legislation to make such protection a reality. Despite Tanzania's efforts to protect children through various legislative and policy initiatives, such initiatives still fall short of tackling the drawbacks brought up by the online ecosystem. The Personal Data Protection Act, the Cyber Crime Act, the Child Act and the Electronic and Postal Communication Act contain several loopholes that allow the violation of children's privacy in cyberspace. For example, in all these laws there is no requirement for internet service providers to implement age verification mechanisms. Therefore, the need for Tanzania to update its legal and policy structure on children's protection online emerges. Additionally, while it may be acknowledged that the adequate safeguard to children's rights largely hinges on the inclusion of all main partakers, children placed at the centre, their involvement in Tanzania has been minimal resulting in the formulation of laws that are not informed with the realities on the ground. It is thus argued that, in a bid to enhance its legal protection for children's rights, Tanzania needs to take on

168 [2017] eKLR.

169 NC Breen 'An analysis of the role of the courts in selected child protection cases: Jurisprudence and remedy' Master's dissertation, University of Pretoria, 2017 6.

board all key stakeholders and formulate laws that incorporate international best practices and standards, ensuring that children in Tanzania enjoy the same level of privacy as their peers worldwide. Cross-border cooperation is also essential especially when the violation has international implications. TCRA is also urged to observe the statistical growth of children's involvement in cyberspace. Considering the sensitive nature of children's online privacy and the essence of safeguarding it, tracking their navigation trends in cyberspace is paramount.

African Journal on Privacy & Data Protection

To cite: GA Arowolo 'Safeguarding the rights to privacy and digital protection of children in Africa: Nigeria and South Africa in focus' (2025) 2
African Journal on Privacy & Data Protection 126-152
https://doi.org/10.29053/ajpdp.v2i1.0007

Safeguarding the rights to privacy and digital protection of children in Africa: Nigeria and South Africa in focus

*Grace Ayodele Arowolo**
Associate Professor and Acting Head, Department of Public and Private Law, Lagos State University, Ojo, Lagos, Nigeria

Abstract

In its General Comment 25 (2021), the United Nations Committee on the Rights of the Child encourages state parties to ensure the protection and upholding of children's rights on the internet. To achieve this, a strong legislative framework is required. Therefore, this article aims to examine the degree to which children's rights to privacy and data protection are incorporated and enshrined into the Nigerian and South African regulatory frameworks. These countries are state parties to various regional and international laws that safeguard the rights of children. The article also aims to explore relevant legislation in the European Union (EU) and the United States of America, as both are assumed to contain comprehensive provisions for protecting the right to privacy of children and protection from online abuse. The purpose is to compare the US and EU laws with the Nigerian and South African laws, detect deficiencies and/or best practices, and the key regulatory and implementation challenges of their legal frameworks. The article adopts a doctrinal approach that enables the analysis of

* BL (Lagos) LLB (Hons) (Ife, Ile Ife) LLM (Lagos State University) PhD (Ambrose Alli); ayodelearowolo2006@yahoo.com; grace.arowolo.edu.ng

various applicable international, regional and national legal frameworks in South Africa and Nigeria. The article finds, among others, that, although both countries have made notable progress in enacting laws safeguarding the rights of children offline and online, the legal frameworks of these countries do not adequately safeguard children's rights to privacy in the online ecosystem. The article argues that with weak legislation, the effective protection of children's right to privacy and their participation in the digital space may be negatively affected. Hence, a reform of the relevant laws is crucial in the two countries, and children should be consulted in the process as they possess the statutory right to be engaged in issues that concern them.

Key words: children; right to privacy; digital protection; Nigeria; South Africa

1 Introduction

In the modern digital age, numerous daily activities produce data, often without immediate awareness. In addition to the information shared, additional data is collected via sensors or derived using advanced algorithms.[1] This circumference results in a complex interplay between digital data processing and the freedoms designed to uphold the right to personal data protection and the right to privacy.[2] While digital technologies provide new avenues for exercising human rights, they are frequently abused to infringe upon human rights generally. Key concerns include digital identity, the use of surveillance technologies, data protection and privacy, and online violence and harassment.[3]

The internet and mobile technologies are a vital aspect of many children's lives.[4] Globally, 79 per cent of individuals aged between 15 to 24 use the internet.[5] In affluent and developing countries, and progressively in lower-income nations, children's activities are increasingly reliant on mobile and online networks, making it nearly impossible to distinguish between online and offline experiences.[6] This integration of offline and online experiences brings about a variety of digitally-driven risks and opportunities.[7] While some have emerged in the digital era, most are influenced by children's inherent needs, abilities, and

1 C Caglar 'Children's right to privacy and data protection: Does the article on conditions applicable to child's consent under the GDPR tackle the challenges of the digital era or create further confusion?' (2021) 12 *European Journal of Law and Technology* 1-31.

2 S Livingstone, M Stoilova & R Nandagiri 'Children's data and privacy online: Growing up in a digital age: An evidence review' (2019), https://eprints.lse. ac.uk/id/eprint/101283 (accessed 5 June 2024).

3 I Milkaite & E Lievens 'Children's rights to privacy and data protection around the World: Challenges in the digital realm' (2019) 10 *European Journal of Law and Technology* 1-24.

4 M Stoilova, S Livingstone & D Kardefelt-Winther 'Global kids online: Researching children's rights globally in the digital age' (2016) 6 *Global Studies of Childhood* 455-466.

5 International Telecommunication Union (ITU) 'Facts and Figures 2023', https://www.itu.int/itu-d/reports/ statistics/ 2023/10/10/ ff23-youth-internet-use/#:~:tex (accessed 4 July 2024).

6 Livingstone and others (n 2).

7 EJ Helsper and others 'Country classification: Opportunities, risks, harm and parental mediation' (2023), https://eprints.lse.ac.uk/52023/ (accessed 24 July 2024).

susceptibilities.[8] The emergent opportunities for children include the utilisation of new recreational and social media as sites of learning, including peer-based learning; the accumulation of social and technological skills for participation in today's world; and variety in media literacy and online engagements, which may offer advantages for socialisation and education, preparing individuals for future social and professional environments.[9] Most of the risks that children might encounter relate to social media violence such as sexual predation and grooming, cyberbullying, 'sexting' and harassment.[10]

Thus, the digital era has created both challenges and opportunities in advancing children's rights worldwide.[11]

Threat to children online constitutes an infringement on their privacy and protection from abuse and exploitation.[12] Children are more susceptible to interferences in their privacy because of their inability to comprehend the long-term effects of disclosing personal data online.[13] Further to the foregoing, children seek assurances against commercial exploitation and have urged governments to enact laws that safeguard their information and limit industry monitoring of minors online.[14] Several years earlier, Livingstone and others advocated a new General Comment from the United Nations (UN) Committee on the Rights of the Child (CRC Committee). This is as a result of the risks children face in online environments and the vast opportunities they may be denied, the rapidity of change and the fact that 'digital' is not about to go away.[15]

Consequently, in 2021 the CRC Committee adopted General Comment 25, which explains how state parties should enforce the Convention on the

8 L Raftree & K Bachan 'Integrating information and communication technologies into communication for development strategies to support and empower marginalised adolescent girls' (2013), https://www.Researchgate.net/publication/330135273_Integrating_Information_and_Communication_Technologies_into_Communication_for_Development_Strategies_to_Support_and_Empower_Marginalized_Adolescent_Girls?. (accessed 20 July 2024).

9 C Samuels and others 'Connected dot com: Young people's navigation of online risks: Social media ICTs and online safety' Cape Town, South Africa: Centre for Justice and Crime Prevention and UNICEF (2013) 11-12.

10 As above.

11 I Milkaite & E Lievens 'The internet of toys: Playing games with children's data?' in G Mascheroni & D Holloway (eds) *The internet of toys: Practices, Affordances and the political economy of children's smart play* (2019) 285.

12 OM Sibanda 'Protection of children's rights to privacy and freedom from online exploitation and abuse in Southern Africa: A case study of South Africa and Zimbabwe' Master's dissertation, University of Pretoria, 2019/2020 2.

13 UNICEF 'Children's online privacy and freedom of expression' (2018), https://www.guvenliweb.org.tr/dosya/ ZybsG.pdf (accessed 15 May 2024).

14 A Third & L Moody 'Our rights in a digital world: A report on the children's consultations to inform UNCRC General Comment 25' (2021), https://5rightsfoundation.com/uploads/OurRIghtsinaDigitalWorld-FullReport.pdf (accessed 23 May 2024).

15 S Livingstone, G Lansdown & A Third 'The case for a UNCRC General Comment on children's rights and digital media' Report prepared for Children's Commissioner for England, 28 June 2017, London School of Economics (LSE) 1-63.

Rights of the Child (CRC),[16] pertaining to the digital landscape.[17] CRC is the first international instrument with legally binding force to encompass the comprehensive scope of children's human rights.[18] These include the right to privacy (article16); the right to attain and enjoy the highest possible standard of health (article 24); the right to an adequate standard of living that supports the child's social, mental, physical, and spiritual development (article 27); and the right to education (article 28).

General Comment 25 addresses, among other things, the general principles of CRC, that is, the rights of children to equal treatment provided in article 2 of CRC; the child's utmost welfare in article 3; the right to survival, life and development in article 6; and the recognition of the child's perspectives in article 12. The General Comment advanced other rights enshrined in CRC, such as the right to privacy in article 16 of CRC; freedom of expression in article 13; and protection from commercial exploitation in article 32.

One of the measures proposed by the General Comment is for state parties to 'review, adopt and update national legislation in line with international human rights standards, to ensure that the digital environment is compatible with the rights set out in the Convention'.[19]

This article seeks to address how well South Africa and Nigeria have adhered to the recommendations of General Comment 25. The article establishes that the regulatory frameworks of Nigeria and South Africa do not effectively safeguard children's right to privacy and protection from online abuse and exploitation. Hence, the article recommends law reform. The article draws best practices from the legal regimes of the European Union (EU) and the USA to inform law reform. It also makes other recommendations.

2 Understanding the concept of privacy and data protection

Privacy is a basic right crucial for human dignity and autonomy, functioning as the cornerstone for many other rights.[20] It enables the creation of limitations and management of thresholds for protection from unjustified intrusion into people's lives.[21] Data protection is typically defined as legal provisions aimed at

16 Adopted by General Assembly Resolution 44/25 of 20 November 1989.
17 UN Committee on the Rights of the Child General Comment 25 on children's rights in relation to the digital environment' (2021) UN Doc CRC/C/CG/25 dated 2 March 2021.
18 UNICEF 'A summary of the rights under the Convention on the Rights of the Child', https://www.unicef.org/ montenegro/en/reports/summary-rights-under-convention-rights-child, (accessed 5 January 2025).
19 UNICEF (n 18) para 23.
20 Privacy International 'What is privacy', https://privacyinternational.org/explainer/56/what-privacy (accessed 24 June 2024).
21 As above.

safeguarding personal information.[22] A robust data protection framework can empower individuals, curb harmful data practices and prevent data exploitation, playing a crucial role in establishing effective governance structures both nationally and globally.[23]

Article 16 of CRC prohibits the illegal intrusion into children's family life, privacy, home, or communications, and illegal assaults on their reputation and honour. Although a right to 'data protection' is not clearly stated in article 16, General Comment 25 aims to broaden and guide the interpretation of the article provision in CRC.

General Comment 25 summarised the importance of Children's right to privacy in the online space as follows:[24]

> Privacy is vital for children's agency, dignity and safety, and for the exercise of their rights. Threats to children's privacy may arise from their own activities in the digital environment, as well as from the activities of others, for example by parents' sharing online the photos or other information of their children, or by caregivers, other family members, peers, educators or strangers. Threats to children's privacy may also arise from data collection and processing by public institutions, businesses and other organizations; as well as from criminal activities such as hacking and identity theft.

3 Opportunities and risks relating to children's participation online

Digital technology is often regarded as a major game changer of our time, with the potential to transform the lives of the most underprivileged and at-risk children of the world by enabling them to grow, learn, and reach their full potential.[25] Digitalisation enables children with disabilities to interact with others and make independent choices, grants access to education for those in marginalised or remote places and, in humanitarian crises, assists displaced children in finding safe routes and reconnecting with their families.[26] Increased digital connectivity among children has created fresh opportunities for civic participation and social integration, offering the possibility of disrupting cycles of poverty and deprivation;[27] furthers the promotion of their right to education[28]

22 Privacy International 'A guide for policy engagement on data protection: Data protection explained', https:// privacyinternational.org/sites/default/files/2018-09/Part%201%20%20Data%20Protection%2C%20Explained.pdf (accessed 30 June 2024).
23 As above.
24 General Comment 25 (n 17) para 108.
25 UNICEF 'The state of the world's children 2017: Children in a digital world' (2017), https:// www.unicef.org/ media/48581/file/SOWC_2017_ENG.pdf (accessed 12 August 2024).
26 As above.
27 As above.
28 S Livingstone, J Carr & J Byrne, 'One in three: Internet governance and children's rights' Innocenti Discussion Paper 2016-01 United Nations Children's Fund UNICEF 1-36.

and freedom of expression;[29] grants them access to information important for their well-being, including their reproductive and sexual health;[30] grants them the opportunities to develop skills in coding, creating, and sharing information and such opportunities as are available on the internet.[31] Children can also play games, listen to music and watch movies online, thereby enjoying their right to leisure and recreation.[32]

However, It is crucial to emphasise the digital divide, which has prevented some children from benefiting from the advantages provided by the internet for different reasons.[33] According to the United Nations Children's Fund (UNICEF), strong inequality in digital connectivity is evident globally and across the world's regions.[34] Based on 2023 statistics, 98 per cent of youths (individuals aged between 15 to 24 years) in Europe have access to the internet, while in Asia Pacific, 81 per cent of youths, also between ages 15 and 24, have home internet connectivity.[35] However, only 53 per cent of youths aged between 15 and 24 in Africa can access the internet.[36] African children encounter multiple intersecting challenges, such as financial limitations, restricted online literacy, and issues linked to gender and race.[37] For example, in Nigeria, adolescent girls have limited modern employment skills and fall behind in internet access and usage (21 per cent compared to 38 per cent for boys),[38] although both added together remain low.

Although internet access has created opportunities for children, it also poses risks of violating their rights online.[39] One of the major risks confronting children in the online space is the infringement of their right to privacy and protection from exploitation and abuse[40] by the use of technologies through tracking, broadcasting and monitoring children's live images, locations or behaviours.[41] Image-based abuse, cyberbullying and exposure to inappropriate content or harmful advice can lead to negative experiences, including disconnection from

29 Livingstone and others (n 15).
30 As above.
31 As above.
32 Sibanda (n 12).
33 As above.
34 UNICEF & International Telecommunication Union (ITU) 'How many children and young people have internet access at home? Estimating digital connectivity during the COVID-19 pandemic' UNICEF New York, 2020.
35 International Telecommunication Union (ITU) 'Facts and figures 2023', https://public.tableau.com/app/profile/ ituint/viz/ITUFactsandFigures2023/InternetUse05 (accessed 3 January 2025).
36 As above.
37 African Children's Committee 'Day of general discussion: Children's rights in the digital world – A concept note', https://www. acerwc. africa/en/article/activity/day-general-discussion-childrens-rights-digital-world (accessed 24 November 2022).
38 UNICEF 'Country office annual report 2022: Nigeria – 321', https://www.unicef.org/media/142201/file/Nigeria-2022-COAR.pdf (accessed 25 June 2024).
39 Council of Europe Commissioner for Human Rights 'Protecting children's rights in the digital age: An ever-growing challenge' (2014), www.coe.int/en/web/commissioner/-/protecting-children-s-rights-in-the-digital-world-an-ever-growing-challen... (accessed 24 May 2024).
40 Sibanda (n 12).
41 UNICEF 'Children's online privacy and freedom of expression' (Industry toolkit, UNICEF 2018) 8, www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf (accessed 24 May 2024).

reality, emotional distress, anxiety, depression, suicidal thoughts, sexual or physical assault, self-harm and reputational damage.[42]

4 Analysis of states' responsibilities under CRC according to states' interpretation of General Comment 25

General Comment 25 was adopted in the realisation that the digital environment plays a crucial role in various aspects of children's lives, including periods of crisis, as well as in societal functions such as governmental services, commerce and education, which increasingly depend on digital technologies.[43] The General Comment expatiates on the specific positive obligations of states in safeguarding children's rights in online space, including updating or enacting legislation, implementing all-encompassing strategies and policies, and enabling autonomous oversight and investigations by national human rights agencies, and the enforcement of mechanisms to safeguard children from risks, including cyber aggression and online and child sexual abuse and exploitation facilitated by technology.[44]

Article 16 of CRC provides for privacy rights of children as discussed above. The CRC Committee outlines how state parties should apply the Convention in online spaces and offers guidance on policy, legislative, and other mechanisms to ensure absolute compliance with their duties under the Convention and its Optional Protocols. This guidance considers the risks, challenges and opportunities involved in promoting, protecting, fulfilling and respecting all children's rights in online spaces.[45]

The most extensive section in General Comment 25 focuses on the right to privacy. Paragraph 67 of General Comment acknowledges the fact that 'threats to children's privacy may arise from data collection and profiling by public institutions, businesses and other organisations', but equally 'from the activities of family members, for example, by parents sharing photographs online or a stranger sharing information about a child'.

Paragraph 68 highlights various online activities that depend on data processing, including compulsory identity authentication, profiling, extensive monitoring and behavioural targeting. The Committee believes that these practices may result in unlawful or arbitrary infringements on the privacy rights of children. With respect to states' obligations to uphold the privacy rights, paragraph 70 of General Comment 25 states that states must enact and implement data protection laws that include exclusive safeguards for children

42 D Mitra 'Keeping children safe online: A literature review' (2020) Centre for Excellence in Child and Family Welfare Melbourne 1-21.
43 General Comment 25 (n 17) para 3.
44 General Comment 25 (n 17) paras 22-49.
45 General Comment 25 (n 17) para 7.

while ensuring that other rights, such as their rights to play and their rights to freedom of expression, are not arbitrarily restricted.[46]

General Comment 25 also advocates a legal prohibition on specific online activities, such as neuromarketing, consumer-specific advertising and commercial profiling.[47] It acknowledges the duty of states to provide adequate guidance and support to caregivers and parents in fulfilling their child-upbringing obligations. This necessitates the advancement of awareness raising[48] and educational programmes that provide information on protecting children's privacy, targeting several stakeholders, including care givers, parents, children, policy makers and the general public.

The General Comment also emphasises the necessity to respect children's developing capabilities and independence, urging states to support parents in upholding a reasonable balance between their duties and the child's rights.[49] Parents and care givers should be guided in this balancing process by the best interests of the child and the recognition of their evolving capabilities. States are urged to educate care givers, parents, children and the public on the significance of the privacy rights of a child and how certain parental actions may violate this right. When care givers and parents monitor a child's online activities, they should do so proportionately and with utmost regard for the child's evolving capabilities.[50]

5 African regional framework

5.1 African Charter on the Rights and Welfare of the Child

Just like article 16 of CRC, article 10 of the African Charter on the Rights and Welfare of the Child (African Children's Charter)[51] protects children's rights to privacy, home or correspondence, reputation and honour. A major departure of this provision from CRC is the inclusion in its article 10(3) the provision that 'parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children'. However, this was clarified by the African Committee of Experts on the Rights and Welfare of the Child (African Children's Committee) in its General Comment on article 31 of the African Children's Charter espousing that the rationale for the provision is to balance the authority exercised over children by adults with children's responsibility to show respect

46 As above.
47 General Comment 25 (n 17) para 42.
48 General Comment 25 (n 17) para 21.
49 General Comment 25 (n 17) para 86.
50 General Comment 25 (n 17) para 76.
51 OAU/CAB/LEG/153/Rev 2 1990. Nigeria ratified the African Children's Charter on 23 July 2001.

and consideration for that authority.[52] The General Comment further states that the 'rights of the child including freedom of expression, participation, and development, among others, shall not be compromised or violated by reference to "respect for adults"'.[53] Thus, it is essential to recognise that privacy rights of children should not be compromised or infringed upon due to the provision on parental control in article 10(3).[54] The African Children's Charter did not make any provisions for data protection.

5.2 African Union Convention on Cyber Security and Personal Data Protection

The African Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention) is Africa's first regional framework on data protection.[55] Article 8(1) of the Convention mandates state parties to enact regulatory frameworks that reinforce basic rights and freedoms, especially data protection, and to impose sanctions for any breach of privacy.[56] Under article 8(2), any form of data processing should respect basic rights and freedoms. The Convention contains no provision for the handling of data concerning children, but article 29(3) guarantees safeguarding children from exploitation and abuse in online spaces while urging state parties to criminalise child pornography. Article 29(3) provides as follows:

> State parties shall take the necessary measures to ensure that, in case of conviction, national courts will give a ruling for confiscation of materials, equipment, instruments, computer program, and all other devices or data belonging to the convicted person and used to commit any of the offences mentioned in the Convention including child pornography.

Nigeria is not yet a party to this Convention, while South Africa is a signatory.

5.3 Southern African Development Community Model Law on Data Protection and Information and Communications Technology 2013

The law upholds children's privacy as it provides that the personal data of a child can be processed only in accordance with article 37 of the Model Law, which states that 'if a child is the data subject, his or her rights may be exercised by his

52 African Children's Committee General Comment on article 31 of the African Charter on the Rights and Welfare of the Child on the responsibilities of the child' (2017) African Union Commission, Addis Ababa, Ethiopia 1-34.

53 As above.

54 A Singh & T Power 'Understanding the privacy rights of the African child in the digital era' (2021) 21 *African Human Rights Law Journal* 99-125.

55 O Babalola 'Data protection legal regime and data governance in Africa: An overview' (2023) AERC Working Paper DG-003 African Economic Research Consortium, Nairobi, Kenya 1-27.

56 Adopted by the 23rd ordinary session of the Assembly held in Malabo, Equatorial Guinea 2014. Nigeria has neither signed nor ratified the Convention. South Africa signed the Convention on 16 February 2023 but is yet to ratify it.

or her parents or legal guardian' except as per national laws, the child has the capacity to give consent individualistically according to their ability and age, in line with internationally accepted standards that require recognising the evolving capabilities of children. This provision complies with the African Children's Charter discussed above and paragraphs 70 and 71 of the General Comment which interprets CRC.

5.4 African Union Child Online Safety and Empowerment Policy 2024

This policy seeks to identify gaps and areas requiring harmonisation to uphold children's rights and to address cross-border challenges.[57] The goals of the policy include enhancing and harmonising national, regional and continental legal and regulatory frameworks on online safety of children; recognising the advantages of, and responses to, current and growing threats to children's identity, privacy, and agency in the online space; and developing a unified multi-stakeholder framework to address online risks for children, particularly child sexual abuse and exploitation.[58]

The policy's key recommendations include reinforcing high-level governmental commitments to child online safety; enhancing criminal justice systems to enhance law enforcement and for the judicial arm of governments to effectively combat child online safety offences including exploitation and sexual abuse of children in online spaces; and advancing and advocating accessible digital education in schools and among guardians, parents and community stakeholders.[59]

6 Compliance with General Comment 25 recommendations on the right to privacy: Nigeria and South Africa

This part examines the degree to which children's rights to privacy are protected in the digital environment in Nigeria and South Africa, based in light of the provisions of paragraph 70 of General Comment 25 concerning the obligations imposed upon states to adopt robust legislation that safeguards children's right to data protection and privacy.

At the international level, the origin of the right to privacy has been traced to the Universal Declaration of Human Rights (Universal Declaration).[60] Article 12 of the Declaration prohibits the subjection of anyone to the illegal interference with their privacy. Article 17 of the International Covenant on Civil and Political

57 Adopted by the 44th ordinary session of the African Union Executive Council in February 2024 in Addis Ababa, Ethiopia.
58 As above.
59 As above.
60 Universal Declaration of Human Rights 1948.

Rights (ICCPR)[61] forbids arbitrary interference with citizens' privacy. Apart from CRC examined above, these international laws do not make specific mention of children's data protection rights.

7 Nigeria's legal framework

Nigeria is bound by the provisions of the Universal Declaration on right to privacy and is also a party to ICCPR. Other laws and regulations that impact on data protection and privacy in Nigeria include CRC, the African Children's Charter and the General Comment discussed above, as well as the following:

7.1 Constitution of Nigeria

Section 37 of the Nigerian Constitution guarantees 'the privacy of citizens (children inclusive) to their homes, correspondence, telephone conversations and telegraphic communications'.[62] In *Nwali v Ebonyi State Independent Electoral Commission*[63] the Nigerian Court of Appeal broadly interpreted this provision to encompass all facets of human life, thus, tracing the origin of data protection in Nigeria to the privacy provisions guaranteed by the Nigerian Constitution.[64]

With specific reference to privacy rights of children, Nigeria is also a party to CRC[65] and the African Children's Charter[66] which were domesticated to the Child's Right Act (CRA) in 2003.[67] Section 8 of the CRA states that '[e]very child has the right to his privacy, family life, home, correspondence, telephone conversation and telegraphic communications'. As in the African Children's Charter, section 8(3) of the CRA subjects the exercise of children's right to privacy to adequate supervision and oversight by their parents and legal guardians. The provisions of these instruments, including the Constitution, make no specific reference to the safeguarding and respect for children's privacy in the online space.

7.2 Nigerian Data Protection Act 2023

One of the major objectives of the Nigerian Data Protection Act (NDPA) in its section 1 is to protect the basic rights, interests and freedoms of data subjects, as enshrined in the Constitution of the Federal Republic of Nigeria, 1999 (as

61 General Assembly Resolution 2200A (XXI) 1966.
62 Constitution of the Federal Republic of Nigeria 1999 (as amended).
63 (2014) LPELR – 23682 (CA).
64 O Babalola 'Nigeria's data protection legal and institutional model: An overview' (2022) 12 *International Data Privacy Law* 41-52.
65 Adopted by General Assembly Resolution 44/25 1989. Nigeria ratified CRC on 19 April 1991.
66 African Children's Charter (n 51).
67 Child's Right Act 26 of 2003.

amended). Under section 65 of the Act, a child is an individual under the age of 18 years.[68] According to sections 31(1) and (2) of the Act, when the data subject is a child or an individual without legal competence to give consent, the data controller must obtain consent from the legal guardian or parent, as applicable, before processing the child's data. Furthermore, the data controller must implement appropriate procedures to confirm consent and age, taking into account the available technology. However, under section 31(5) of the Act, the Nigeria Data Protection Commission (NDPC) is empowered by the NDPA to establish regulations for protecting children aged 13 and above in relation to accessing information and services electronically upon the explicit request of the child.[69] Thus, with respect to the processing of data from children in the age group of 13 years and above but under the age of 18, guidelines need to be issued from the regulatory agency since, as stated in section 64 of the NDPA, regulations established before the NDPA came into effect shall remain valid unless they conflict with the NDPA or are repealed.[70] This implies that, if a child is above the age of 13, the recommendation of the General Comment would apply. This means that, when a child is mentally matured to understand the consequences of online activities and able to give consent, they can be allowed to give such consent with or without their legal guardian. Section 65 is the definition section of the Act.

The NDPA currently is the primary legislation on data protection in Nigeria, superseding the NDPR. The NDPA will prevail in the event of any conflict with any other regulations.

7.3 Cybercrimes (Prohibition, Prevention, etc) Act 2015

Some of the sections of this Act have been amended by the Cybercrimes (Prohibition, Prevention etc) (Amendment) Act 2024 but the provision on child pornography remains intact. The Act safeguards children against child pornography and other related offences. Section 23 of the Act prohibits the procurement, production, transmission, possession and distribution of child pornography in any data storage device or a computer system, making such actions as offences. Upon conviction, the penalty for such actions is a 10-year prison term or a fine of N20 000 000.00 or both. In contrast, obtaining child pornography for oneself or another person, as well as owning child pornography on a data storage medium or in a computer system, carries a maximum penalty of five years' imprisonment or a fine of up to N10 000 000.00 or both.

Section 23(2) prohibits and penalises soliciting, grooming or proposing, via any computer network or system, to meet a child with the intention of having

68 This is in accordance with the definition of a child in sec 277 of the Child's Right Act.
69 Sec 31(5) NDPA 2023.
70 Sec 64(2)(f) NDPA.

sexual relations with the child. Likewise, the Act punishes the production, transmission, distribution or ownership of child pornography. This implies that sexual conversations with a minor, luring a minor into engaging in child pornography, or committing other acts that aim to exploit a child in the digital space, constitutes a violation of the child's rights, which can be enforced against the perpetrator.[71] However, section 23 of the Cybercrimes Act 2015 did not specifically mention children's rights to privacy in the digital space.

In Nigeria, the legislative framework regulating a child's right to digital privacy is still imperfect. Although there are laws governing general data protection of citizens, children are scarcely mentioned and the few provisions on children are not comprehensive compared to other jurisdictions discussed below. There are other laws, although not primarily focused on data protection, that contain provisions that influence and govern data protection in specific contexts,[72] namely, the Freedom of Information Act 2011;[73] the National Health Act 2014;[74] the HIV and AIDS (Anti-Discrimination) Act 2014; and the National Information Technology Development Agency Act 2007.[75] However, it does not specific provision for privacy rights of children in the digital world.

8 South Africa's legal framework

Just like Nigeria, South Africa is bound by the Universal Declaration and ICCPR. South Africa is a party to CRC[76] and the African Children's Charter.[77] The relevant national laws include the following:

8.1 The Constitution

The right to privacy is generally recognised as a basic human right in the Bill of Rights of the Constitution of South Africa.[78] Section 14 of the Constitution provides for everyone's right to privacy, including 'the right not to have (a) their person or home searched; (b) their property searched; (c) their possessions seized; or (d) the privacy of their communications infringed'. Section 28 safeguards children's rights and the paramountcy of their best interests in every matter that affects them. Section 14 applies to children and is broad enough to include their privacy right in the digital realm as it states 'communication'.

71 MB Adisa 'A child's right in the digital environment: Legal considerations', https://www.mondaq.com/nigeria/privacy-protection/1285096/a-childs-right-in-the-digital-environment-legal-considerations (accessed 15 January 2025).
72 ICLG 'Data protection laws and regulations in Nigeria 2024-2025', https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria (accessed 12 July 2024).
73 CAP F43 Laws of the Federation of Nigeria 2011.
74 Act 8 of 2014.
75 Sec 6(c) Cap N156 Laws of the Federation of Nigeria 2010.
76 CRC (n 16). South Africa ratified the Convention in 1995.
77 African Children's Charter (n 51). South Africa ratified the Charter in 2000.
78 The Constitution of the Republic of South Africa, 1996.

8.2 Children's Act 38 of 2005

The Children's Act[79] complements the rights of children enshrined in the South African Constitution. Section 1 defines abuse to include bullying, sexual abuse and subjecting or exposing a child to actions that may be detrimental to them. The section further defines commercial sexual exploitation as the recruitment of a child to engage in sexual activities in exchange for money or other rewards, including pornography and prostitution. These forms of abuse though not explicitly addressed defined in the Act can be linked to harmful acts perpetrated on the internet.

The Children's Act 38 of 2005 is currently being amended to better align with the data protection and privacy rights of children in South Africa.[80] This is a specific requirement of the General Comment on children's privacy protection in the online space. It is hoped that the amendment will be finalised.

8.3 Protection of Personal Information Act

The objectives of the Protection of Personal Information Act (POPIA) include the advancement and safeguarding of personal information processed by private and public entities and the Promotion of Access to Information Act, 2000.[81] Section 34 of the Act forbids the processing of personal data of children by any responsible party except as stated under section 35 when, among others, the processing is conducted with the prior consent of a competent individual; it is essential for the enforcement, exercise, or protection of a legal right or duty; required to abide by an obligation under international public law; or intended for research, statistical, or historical purposes. From the above provisions, it is clear that the Act does not permit the handling of personal information of another person without their consent and provides stringent, additional protection to children in section 35. However, section 35 also creates a limitation as to when children's data may be processed. It can be assumed that where the processing of information is not one of the exceptions listed in section 35, the personal information of a child cannot be allowed for processing. It has also been posited that there is still significant uncertainty regarding how POPIA will regulate the processing of children's information.[82]

79 Children's Act 38 of 2005.
80 Centre for Human Rights *A study on children's right to privacy in the digital sphere in the African region* (2022) 1-57.
81 Protection of Personal Information Act 4 of 2013 (POPIA).
82 POPIpack 'Unpacking the processing of children's information in terms of POPI', https://www.popipack.co.za/unpacking-the-processing-of-childrens-information/ (accessed 12 January 2025).

8.4 Films and Publications Amendment Act 2019

The aims of the Act include the amendment of the Films and Publications Act, 1996, in order to amend and insert certain definitions; make provision for the composition, establishment and selection of members of the Enforcement Committee; expand the compliance obligations under the Films and Publications Act, along with the adherence and oversight responsibilities of the Film and Publication Board, to include online distributors; strengthen the regulation of the classification of games, publications, and films; and provide for accreditation of independent commercial online distributors by the Film and Publication Board.[83]

Section 18(G)(1) criminalises the production, creation or distribution by any person 'in any medium, including the internet, and social media any films or photographs depicting sexual violence and violence against children'.[84] It is an offence under section 24(A)(4)(a) and section 24(3)(j) for anyone to permit children access to a game, publication, or film rated 'X18', including granting children access to scenes of explicit sexual conduct. Furthermore, registered film or game distributors may, provided an exemption is granted by the South African Film and Publication Board, distribute a game or film classified as 'X18' online, subject to conditions such as ensuring that children are unable to access such a game or film online. Section 24B criminalises child pornography.[85]

8.5 Criminal Law (Sexual Offences and Related Matters) Amendment Act 2007

This Act makes comprehensive provision for children's protection against sexual offences, including offences related to grooming or sexual exploitation, and the production of child pornography, although the offences are similar to the offences created for adults, with the aim of addressing the particular vulnerability of children.[86] Section 10 prohibits and criminalises the display or exposure of child pornography to adults, while section 19 criminalises the exposure or display of child pornography to children. Sections 17 and 18 prohibit the sexual exploitation of children for monetary or other gain and grooming of children respectively. Under section 20, it is also a crime to derive a benefit from or use a child for child pornography. However, the Act has been criticised for creating sexual offences that largely overlap with those created in the Films and Publications Act.[87] The provision of the Criminal Law Amendment Act, however,

83 The Films and Publications Amendment Act 11 of 2019.
84 As above.
85 As above.
86 Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007.
87 SS Terblanche & N Mollema 'Child pornography in South Africa' (2011) 24 *South African Journal of Criminal Justice* 286.

is acceptable since the aims and objectives of the Act are different from that of the Films and Publications Act.

8.6 Cybercrimes Act 2020

In terms of section 3 of the Cybercrimes Act,[88] the illegal interception of data is an offence, while the unlawful distribution of data messages is an offence under section 14. Section 15 also makes it an offence for a person to make an unlawful and intentional data message that threatens persons with damage to property or violence. Section 24 of the Act gives South African courts jurisdiction over any act or omission alleged to constitute an offence under the Act and that affects an individual in South Africa, even if the defined cybercrime occurs outside the country.

Pursuant to the Cybercrimes Act, litigations involving children's protection have been brought before the courts. For example, in *SM v ABB*[89] the father of the child had shared content from her WhatsApp chat (as well as her mother's) during a divorce case. The child's mother filed an application to prevent the father (respondent) from further accessing and distributing both her (the applicant's) WhatsApp messages and emails, as well as those of their minor child.

The Court ruled that the respondent's behaviour in accessing the applicant's and the minor child's messages violated their right to privacy: The information was shared with the medical practitioner and the headmaster solely to create a cognitive bias in their minds against the applicant and potentially the minor.

The case indicates that parental rights to access the child's digital communications without justification may be restricted with respect to a child's privacy rights. It also portrays South Africa's efforts in protecting privacy rights online.

Furthermore, in *S v Stevens*[90] the accused, Stevens, was involved with two young girls, who were five years old at the time of the incident. He was accused of removing the underwear of the girls while they were asleep for the purpose of taking photographs, and in certain instances touching their private parts with his fingers. Approximately 71 photographs were taken of the children. He was convicted on two counts of indecently assaulting the girls and eight counts of creating and possessing child pornography in contravention of sections 27(1)(a)(i) and (ii) of the Films and Publications Act 65 of 1996. The regional magistrate handed down a sentence of eight years' imprisonment to the accused, of which three years were suspended. Upon appeal to the High Court of Eastern Cape

88 Cyber Crimes Act 19 of 2020.
89 Case 20/1732 (11 September 2020, Gauteng Local division).
90 (2007) JDR 0637 (E). 188 [2014] 2 SACR. CA & R54/07.

Province, the sentence was modified to six years' imprisonment, with two years suspended.

In *S v Kleinhans*[91] a 74 year-old businessman, Kleinhans, was charged with numerous counts of sexual offences against underaged girls. Most of the charges involved capturing photographs of a complainant, a young girl who was between the ages of 13 and 14 years, while she was either only partially clothed or naked. The appellant was charged with an offence of producing child pornography which he was able to do through producing nude pictures of a child complainant in contravention of section 24(B)(1)(b) of the Films and Publications Act 65 of 1996, and the provisions of the Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007 (the Act) which prohibits, among others, the manufacture of child pornography in section 20(1), sexual grooming of children in section 18(2)(a) of the Act and sexually assaulting the complainant (a child) by fondling her breasts in section 5(1) of the Act.

The magistrate sentenced the accused to 15 years' imprisonment. Upon appeal to the High Court of South Africa, Western Cape Division, the 15-year prison sentence was overturned and substituted with an effective term of imprisonment for four years, with an additional suspension of four years.

South Africa has also made many efforts in adopting policies and laws that recognise the safeguarding of children's privacy online, and has taken a step further by signing the Council of Europe Convention on Cybercrime, the first international treaty on offences committed through the internet and other computer networks.[92] Being an observer to the Convention, South Africa has the privilege and ability to participate in the activities and discussions relating to the Convention without being legally bound. However, it lacks the ability to vote or propose solutions to the challenges of the Convention.[93] South Africa was the sole African nation to take part in the negotiations for the Council of Europe Convention on Cybercrime.[94] Consequently, the South African government has implemented various laws addressing cybercrime and incorporating substantive legal provisions from the Council of Europe Convention.[95] Most notable in this regard is the Electronic Communications and Transactions Act 25 of 2002 (ECT Act), the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013.[96]

91 (2014) 2 SACR.
92 Council of Europe 'Fight against cybercrime' (2015), https://www.europewatchdog.info/en/treaties_and_ monitoring/ cybercrime/ (accessed 12 August 2024).
93 T Reinsman 'International organisations or institutions, observer status', https://opil.ouplaw.com/display/ 10.1093/ law:epil/9780199231690/...(accessed 12 January 2025).
94 Council of Europe 'Cybercrime', https://www.coe.int/en/web/cybercrime/-/octopus-project-benchmarking-the-implementation-of-the-south-african-cybercrimes-act-in-line-with-the-international-best-practice... (accessed 10 January 2025).
95 Council of Europe 'South Africa', https://www.coe.int/en/web/octopus/-/south-africa (accessed 10 January 2025).
96 As above.

Nigeria has acceded to the Council of Europe Convention since 6 July 2022.[97] However, the failure to enshrine digital protection in the extant child right protection laws in Nigeria and South Africa suggests that the countries still have much ground to cover. Therefore, law reform through amendments to existing frameworks to address new risks is hereby suggested.

9 The legal framework for safeguarding children's privacy and data protection in other jurisdictions

For this purpose, the European Union (EU) and the United States of America (USA) have been selected.

9.1 European Union

The EU has been rated as having one of the broadest data privacy protection frameworks globally and is regarded as a pacesetter and catalyst of data privacy protection laws.[98] The data protection framework explicitly acknowledges that processing children's personal data requires special safeguards and offers strengthened protection for such data,[99] although the General Data Protection Regulation (GDPR) of the EU considered below does not specifically provide for their protection 'offline'. Both South Africa and Nigeria also have explicit provisions for safeguarding children online, as examined earlier in this article. The Nigerian NDPA is much more detailed on their online protection than the GDPR. The wording of the provisions of the EU framework is as discussed under the European Union Primary Laws below. European law protecting children's rights is largely based on CRC.[100]

9.1.2 European Union primary laws

The EU provides for the safeguarding of both the right to data protection and right to privacy.[101] First, article 16 of the treaty on the functioning of the EU provides that 'everyone has the right to the protection of personal data concerning them'.[102] Article 7 of the Charter of Fundamental Rights of the European Union 2000 (CFREU) established the citizens' right to privacy by stating that

97 N Ayitogo 'Nigeria signs Budapest Convention on Cybercrime', https://www.premiumtimesng.com/news/top-news/550037-nigeria-signs-budapest-convention-on-cybercrime.html?tztc=1 (accessed 15 January 2025).
98 AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2 *International Data Privacy Law* 163-178.
99 Lexis Nexis 'EU GDPR – Children and data protection law', https://www.lexisnexis.co.uk/legal/guidance/eu-gdpr-children-data-protection-law (accessed 14 January 2025).
100 European Union Agency for Fundamental Rights and Council of Europe *Handbook on European law relating to the rights of the child* (2022) 26.
101 Milkaite & Lievens (n 3).
102 European Parliament 'Understanding EU data protection policy', https://www.europarl.europa.eu/RegData/ etudes/BRIE/2020/651923/EPRS... (accessed 15 January 2025).

'everyone has the right to respect for his or her private and family life, home and communications'.[103] Article 8 recognises the right of everyone to the protection of their personal data, which has to be handled lawfully and fairly for stipulated purposes, either with the person's consent or on another legal basis.

Importantly, article 24 of CFREU expressly recognises the right of the child to protection, essential for their well-being, and to freely share their opinions on issues affecting them, in line with their maturity and age, whereas in all matters involving children, their best interests must be a foremost consideration.[104]

9.1.3 General Data Protection Regulation

The EU adopted a specific provision in the General Data Protection Regulation (GDPR)[105] to tackle issues regarding the processing of children's data.

Under article 1, the subject matter and objectives of the GDPR were stated. It 'lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data'. The GDPR contains several provisions specifically designed to protect the rights of child data subjects. Recital 38 of the GDPR recognises that children require special protection concerning their personal data, given the fact that they may not be as aware as adults of the consequences, risks, safeguards, and their rights regarding data processing. According to the recital, such special protection is particularly essential when collecting children's data for profiling and marketing purposes.[106]

Regarding the lawfulness of data processing, article 6(1)(a) mandates that the data subject gives consent to the processing of their personal data. Under article 8(1) of the Regulation, the processing of the personal data of such child shall be lawful 'where the child is at least 16 years old'. If the child is under the age of 16, this kind of processing must be deemed lawful only 'if consent is given or authorised by the holder of parental responsibility over the child'.[107] Such consent, however, is not required in the context of counselling or preventive services provided directly to a child.[108] By law, member states may provide for a lower age not below 13 years.[109]

103 Charter of Fundamental Rights of the European Union (CFREU) (2000/C 364/01).
104 As above.
105 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 (2016) L 119/1.
106 Milkaite & Lievens (n 3).
107 As above.
108 Recital 38 GDPR.
109 Art 8(1) GDPR.

Article 12 of the GDPR requires the processing of data to be 'concise, transparent, intelligible and in an easily accessible form, for any information addressed specifically to a child'.[110]

Article 17 of the GDPR provides the data subjects with the right to erasure ('right to be forgotten') of personal data concerning them, among others, when the personal data is no longer needed, or the data subject revokes the consent upon which the processing is based or objects to the processing. Generally, article 7(3) of the GDPR states that it 'shall be as easy to withdraw consent as it is to give it'. However, the right to erasure is not absolute and may be overridden, for instance, when required to uphold the right to freedom of information and expression.[111] Its most significant limitations stem from the necessity to balance erasure with freedom of expression and the public interest, as outlined in article 17 of the GDPR.[112]

Similarly, in Nigeria, section 34(1)(d) of the NDPA examined above provides for a data subject's right to erasure, while section 24 of South Africa's POPIA equally provides that there may be a request from a data subject to the controller to amend or remove their personal data. This will be helpful to children whose consent was ignorantly given or who want their information removed for any reason. Generally, however, the GDPR does not specifically provide for their protection 'offline'. Also, both South Africa and Nigeria have explicit provisions for the protection of children online, mentioned in this article. In fact, the Nigerian Act is much more detailed on their online protection than the GDPR.

10 United States of America

The United States adopts a sectoral approach to data privacy regulation, as it lacks an all-encompassing federal law that regulates the privacy and protection of personal data.[113] The statutes are applicable only to specific sectors such as 'healthcare, education, communications, and financial services or, in the case of online data collection, to children'.[114]

110 As above.
111 Information Commissioner's Office 'How does the right to erasure apply to children?', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children... (accessed 15 January 2025).
112 S Grossi 'The right to erasure: To be or not to be, forgotten?', https://www.byarcadia.org/post/the-right-to-erasure-to-be-or-not-to-be-forgotten (accessed 20 January 2025).
113 SM Boyne 'Data protection in the United States' (2018) 66 *American Journal of Comparative Law* 299-343.
114 N Terry 'Existential challenges for health care data protection in the United States' (2017) 3 *Ethics, Medicine and Public Health* 21.

10.1 Children's Online Privacy Protection Act of 1998

Although the United States has not ratified CRC, it adopted the Children's Online Privacy Protection Act (COPPA)[115] in 1998 and has since acquired extensive expertise in implementing it in practice.[116] COPPA governs the collection and use of data collected from children under 13 by websites and mobile applications. Section 1301(1) defines a child as a person below the age of 13. Section 1303 prohibits unfair and deceptive acts for gathering and processing children's personal information online. An operator or online website is required to secure verifiable parental authorisation for collecting, disclosing, or using children's personal information under section 1303(b)(A)(ii) except where the online contact information collected from a child is used solely to respond once (on a singular basis) and directly, to a particular request from the child and is neither retained in a retrievable form nor used for further contact by the operator under section 1303(2)(A), or a request for online contact information or a parent's or child's name, solely for the purpose of securing parental consent under section 1303(2)(B).

10.2 Children and Teens' Online Privacy Protection Act

On 7 July 2024 the US Senate passed the Children and Teens' Online Privacy Protection Act (COPPA 2.0)[117] and the Kids Online Safety Act (KOSA) to better protect teens and children online.[118] The aim is to amend the Children's Online Privacy Protection Act of 1998 to enhance safeguards for the online use, collection and disclosure of personal information of children and teenagers, along with other related objectives. COPPA 2.0 prohibits online companies from obtaining personal information from users under the age of 17 years without their authorisation. It prohibits targeted advertising to teenagers and children and introduces a button to eraser, allowing parents and children to delete personal information online.[119] When in full force, this will aid better protection of children's privacy protection online.

115 The Children's Online Privacy Protection Act (COPPA) is a US federal law that was adopted in 1998 and became applicable in 2000.

116 Milkaite & Lievens (n 3).

117 118th Congress 1st session 'In the Senate of the United States', https://www.markey.senate.gov/imo/media/doc/coppa_20_in_118th_-_050323pdf.pdfhttps://www.markey.senate.gov/imo/media/doc/coppa_20_in_118th_-050323pdf.pdf (accessed 10 August 2024).

118 US Senate Committee on Commerce Science and Transportation 'Senate overwhelmingly passes children's online privacy legislation' Press Release, 30 July 2024, https://www.commerce.senate.gov/2024/7/senate-overwhelmingly-passes-children-s-online-privacy-legislation (accessed 12 August 2024).

119 US Senate Committee on Commerce Science and Transportation 'Kids online privacy protections – finally – set to pass Senate', https://www.commerce.senate.gov/2024/7/kids-online-privacy-protections-finally-set-to-pass-senate (accessed 12 August 2024).

10.3 Children's Internet Protection Act

The Children's Internet Protection Act (CIPA) was passed by Congress in 2000 to address issues regarding children's exposure to harmful or obscene content online.[120] CIPA imposes particular requirements for schools and libraries that receive discounted internet access or internal connections through the E-rate programme, a programme that helps make certain products and communication services more affordable for eligible institutions.[121] Libraries and schools subject to CIPA are ineligible for E-rate programme discounts unless they certify the implementation of an online safety policy incorporating technology protection measures.[122] The protective measures must filter or restrict internet access to images that are (a) obscene, (b) classified as child pornography, or (c) harmful to minors (when accessed on computers used by minors). Schools subject to CIPA must meet two additional certification requirements: (i) their internet safety policies must incorporate monitoring of minors' online activities; and (ii) they must educate minors on proper behaviour when on the internet, including communications on social networking websites, in chat rooms, and awareness of as well as response to cyberbullying.[123]

Libraries and schools subject to CIPA must establish and enforce an internet safety policy that addresses various concerns, including minors' access to indecent online content, their security and safety while using chat rooms, email, and other direct electronic communications, as well as unauthorised access, such as 'hacking' and other illegal online activities by minors.[124]

10.4 The United States Code

The United States Code (USC) is a compilation of a number of public laws presently valid and in force, organised by subject matter. The Code is organised into 54 titles, by subject area, further divided by section and chapter. The US Code also contains provisions for online protection of children in America.[125] The following online activities are prohibited under the US Code:

120 Federal Communications Commission 'Children's Internet Protection Act (CIPA)', https://www.fcc.gov/sites/ default/files/childrens_internet_protection_act_cipa.pdf (accessed 12 August 2024).
121 As above.
122 As above.
123 As above.
124 As above.
125 United States Senate 'The United States Code', https://www.senate.gov/pagelayout/legislative/one_item_ and_teasers/usCode_page.htm (accessed 13 August 2024).

10.5 Sexual exploitation of children (production of child pornography)

Section 2251 title 18 of the Code[126] prohibits the induction, enticement or coercion of a minor to be involved in conduct that is sexually explicit for purposes of creating visual depictions of such conduct. Attempts or conspiracy to commit child pornography is an offence that is subject to prosecution under federal law.[127] Section 2256 defines child pornography as any visual portrayal of sexually-explicit behaviour involving a minor (an individual under the age of 18). Under that section, visual depictions encompass videos, photographs, computer-generated or digital images that are indistinguishable from a real minor, as well as images that have been created, altered or adapted, but appear to show a recognisable, real minor.[128] Under federal law, unprocessed videotape, undeveloped film, and digitally stored data that has the potential to be converted into visual images of child pornography are also considered unlawful visual depictions.[129]

Child pornography attracts stiff penalties. For instance, in *US v James Snyder*[130] the accused was convicted for producing, receiving, distributing and possessing child pornography and sentenced to 168 months' imprisonment followed by six years of supervised release. In *US v Donald Blakley*[131] the accused was convicted on a 15-count charge for conspiracy to knowingly receive and distribute visual portrayals of a minor engaged in conduct that is sexually explicit and sentenced to approximately seven years and three months' imprisonment.

10.6 Cyberbullying

Section 223(a)(1)(B) of title 47[132] makes it an offence to knowingly use a telecommunications device to produce, generate, initiate or solicit the transmission of any comment, proposal request, image, suggestion, or other obscene communication, including child pornography, with the knowledge that the recipient is under 18 years of age.[133] Further, harassing any individual or repeatedly using a telecommunications device to initiate communications with the intent to harass constitutes an offence punishable by up to two years' imprisonment, a fine, or both.[134]

126 Criminal Division US Department of Justice 'Citizen's guide to US federal law on child pornography', https:// www.justice.gov/criminal/criminal-ceos/citizens-guide-us-federal-law-child-pornography (accessed 13 August 2024).
127 As above.
128 As above.
129 As above.
130 (2005) 239 F 229.
131 222 USC sec 2252B(d) title 18.
132 Legal Information Institute (LII) '47 US Code § 223 – Obscene or harassing telephone calls in the district of Columbia or in interstate or foreign communications', https://www.law.cornell.edu/uscode/text/47/223 (accessed 10 August 2024).
133 As above.
134 As above.

10.7 Obscene visual representations of the sexual abuse of children

Section 1466A of title 18[135] prohibits any person from knowingly creating, receiving, possessing or distributing with the intent to transfer or distribute visual representations, including paintings, cartoons or drawings, which depict minors appearing to engage in conducts that are sexually explicit and are considered obscene.[136] Any individual who attempts or conspires to commit the act shall also be deemed guilty of the offence.[137] Section 1470 of title 18 prohibits the transfer or attempted transfer of material that is obscene to a minor who is below the age of 16 using the US mail or any means of foreign or interstate commerce.[138] It is illegal for a person to deliberately use interactive computer services to display obscene material, making it available to a minor below 18 years,[139] and knowingly making a commercial communication through the internet, including obscenity, available to any minor.[140]

10.8 Coercion and enticement

Under section 2422(b) of title 18[141] it is a criminal offence for any individual to knowingly use any facility, the mail or any means of foreign or interstate commerce, or to act within the special territorial or maritime jurisdiction of the United States, to entice, induce or coerce a person under the age of 18 to engage in prostitution or any sexual activity. An attempt to do so is also an offence. Upon conviction, the offender shall be fined and sentenced to a minimum of 10 years' imprisonment or for life.[142]

11 Gaps in the Nigerian and South African legal frameworks

Based on the analysis of the legal frameworks for safeguarding the protection of children's data and privacy online in the EU and the United States, it is observed that some gaps exist in the legal and regulatory frameworks of South Africa and Nigeria.

An overview of the regulatory framework for safeguarding children's privacy rights in Nigeria above indicates that some of the legislations are not adapted

135 Legal Information Institute '18 US Code § 1466A – Obscene visual representations of the sexual abuse of children', https://www.law.cornell.edu/uscode/text/18/1466A... (accessed 11 August 2024).
136 As above.
137 USC sec 1446A(2)(B) title 18.
138 18 USC 1470: 'Transfer of obscene material to minors', https://uscode.house.gov/ view.xhtml?req= granuleid: USC-prelim-title18-section1470&num=0&edition=prelim (accessed 9 August 2024).
139 USC sec 223(d) title 47.
140 USC sec 231 title 47.
141 Legal Information Institute (LII) '18 US Code § 2422 – Coercion and enticement', https://www.law.cornell.edu/ uscode/text/18/2422 (accessed 9 August 2024).
142 As above.

to the digital environment. Although the National Data Protection Act, 2023 regulates the manner of processing of children's data, it is mainly concerned with parental consent without making comprehensive provisions for child's privacy online protection as it exists especially under the US laws considered above.

Despite the foregoing, Nigeria has made much more progress than South Africa through the incorporation of more robust provisions for the protection of children's privacy online via section 31 of the NDPA. Section 31 requires data controller(s) to obtain the consent of the parent or guardian and also verify the age of a child using identification documents approved by government before processing the data of any child. In South Africa, section 35 of POPIA requires that consent of a competent person be obtained before processing a child's data, but unlike the NDPA, it does not explicitly require the responsible party to verify the age of the child. The Nigerian Cybercrimes Act discussed above also safeguards children against child pornography and other related offences. However, the provisions of these laws need to be expanded to comprehensively address the safeguarding of children's data. The expansion can be done through law reform wherein necessary provisions such as in the US laws are incorporated into them. With regard to South Africa, the provisions of the Sexual Offences Legislation and the Films and Publications Act also safeguard children from online abuse and exploitation as they address issues of exploitation of children, child pornography, online grooming and the exposure of children to harmful content. The Protection of Harassment Act also protects children from online harassment. However, both countries, Nigeria and South Africa, still need to take steps to review their laws in line with the recommendations of the CRC Committee's General Comment 25 discussed above, taking inspiration also from the US laws.

12 Recommendations

In order to safeguard the rights to privacy of children and ensure their freedom from online abuse and exploitation, in compliance with General Comment 25, the following recommendations are made:

(1) The existing laws, especially the CRA and NDPA of Nigeria and the Child Law of South Africa, should be reviewed to comprehensively enshrine provisions similar to those in the USA laws so as to come in tune with current global realities in the digital realm, the exposure and the attendant risks posed to children online. This also ensures compliance with General Comment 25's prescription in its paragraph 25. The provisions regulating internet usage in schools as was done in the USA need to be enshrined in Nigerian and South African laws. Obviously, the two countries are not yet parties to the African Union Convention on Cyber Security and Personal Data Protection 2014. Becoming parties can help both countries in reviewing their legislation.

(2) For adequate implementation and enforcement of legislation, it is crucial for both Nigeria and South Africa to mobilise, allocate and utilise public resources, policies and programmes aimed at fully upholding children's rights in the digital environment, enhancing digital inclusion to address the growing impact of the digital world on children's lives, and promoting equal access to affordable services and connectivity. This is in line with paragraph 21 of General Comment 25 which states the obligation of state parties to undertake 'all appropriate measures', including the duty to ensure that laws and policies are established to facilitate resource mobilisation, budget allocation, and expenditure for the realisation of children's rights, and that relevant data and information on children are gathered and disseminated to support the implementation of appropriate legislation, programmes, policies, and budgets aimed at advancing children's rights.[143]

(3) The Nigerian and South African governments should raise public awareness on the importance of children's digital rights and online safety in collaboration with businesses and civil society organisations. In this way, children should be educated on online safety techniques to protect themselves and their personal data in the digital space.[144] This includes providing parents, guardians, teachers and children with appropriate information on child online safety considering their different ages and evolving capacities. The use of local languages and braille is also encouraged for children with disabilities.[145]

13 Conclusion

The analysis in this article has illustrated that children stand to benefit highly from participating online but, at the same time, are exposed to many risks. The article also indicates that safeguarding children's rights to privacy online is not yet explicitly enshrined in both Nigerian and South African children's rights laws, while the general laws do not contain comprehensive provisions. As rightly asserted by Livingstone and others, digital media are no longer luxuries; they are expeditiously becoming essential to modern life globally.[146] Due to the challenge of understanding and managing the digital innovations, governments worldwide, together with organisations dedicated to children's welfare, are advocating a principled, unified and evidence-based framework to acknowledge and uphold the best interests and rights of children.[147] By this, the fulfilment to children of the

143 UN CRC Committee General Comment 19 (2016) on public budgeting for the realisation of children's rights para 21.

144 T Iyoha-Osagie & OI George 'The right to online data protection of children: Examining the adequacy of the legal frameworks in Nigeria' (2019) 3 *ABUAD Private and Business Law Journal* 82-109.

145 UNICEF 'Child safety online: Global challenges and strategies technical report (UNICEF 2012) 78-79, www. unicef-irc.org/publications/652-child-safety-online-globalchallenges-and-strategies-technical-report.html (accessed 13 April 2024).

146 Livingstone and others (n 15).

147 As above.

ethical obligations in this respect is a matter of practical necessity.[148] Therefore, the governments of South Africa and Nigeria must rise up to the task of not only affording children adequate opportunities and means for participation online, but also providing comprehensive legal frameworks for children's privacy safeguard from risks such as cyber-aggression, technology-facilitated harm, online exploitation and child sexual abuse, a recommendation of the CRC Committee's General Comment 25 and practised in the USA.

148 As above.