Raymond Atuguba, Moritz Hennemann, Patricia Boshe and Sena Afua Dei-Tutu
African Data Protection Laws

Global and Comparative Data Law

Edited by
Moritz Hennemann
Lea Katharina Kumkar
Linda Kuschel
Björn Steinrötter

Volume 3

African Data Protection Laws

Regulation, Policy, and Practice

Edited by
Raymond Atuguba
Moritz Hennemann
Patricia Boshe
Sena Afua Dei-Tutu

DE GRUYTER

ISBN 978-3-11-079761-9
e-ISBN (PDF) 978-3-11-079790-9
e-ISBN (EPUB) 978-3-11-079794-7
ISSN 2751-0174
DOI https://doi.org/10.1515/9783110797909

Library of Congress Control Number: 2024930005

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.dnb.de.

Cover image: peshkov / iStock / Getty Images
Printing and binding: CPI books GmbH, Leck

www.degruyter.com

Foreword

Dear fellow reader,

This volume presents the proceedings of the conference on "African Data Protection Laws: Regulation, Practice, and Policy" held in Accra, Ghana. The conference formed the second part of the Global Data Law conference series and took place at the University of Ghana School of Law from 13th to 15th of September 2022. The conference was co-organised by the University of Ghana School of Law and the University of Passau Centre for Law and Digitalisation (FREDI). We tremendously thank the conference speakers – for their in-person presentations in Accra and for taking the time to convert their presentations into a paper format for this volume.

First and foremost, we are deeply thankful for the possibility to bring together data (protection) law experts from within and beyond the African continent in a unique gathering. Hosting an in-person event, with additional participants joining virtually from all around the world, was a distinct privilege. Experts from different jurisdictions generated sharp, thoughtful and lively discussions on the present status, challenges, and future prospects of data (protection) regulation in Africa – from a comparative angle and in view of a Pan-African regulatory framework. The three conference days offered a fantastic chance to exchange views, learn from each other, and contemplate on pressing issues affecting local values, legal cultures, and regulatory development on the African continent.

The conference was made possible by the enormous generous support from the Bavarian State Ministry for Science and Arts, the Germany Embassy in Ghana, the African Digital Rights Hub and the Friedrich Ebert Stiftung Ghana Office. We are more than grateful for this invaluable support which made the conference a huge success.

Finally, we deeply thank the organising teams from Accra (especially Susie Lamptey, Katherine Aglobitse, Nadia Torsu, Benedicta Armah, Clement Addo, Andrew Sackey, the Law Students Union and as well as the excellent conference ushers) and Passau (Johanna Hähnle, Kristyna Zoufala, Josefine Ehrlicher, Timo Hoffmann as well as Julia Lebmann and Sinah Tatschke) without whom the conference would never have taken place.

Accra and Passau, March 2023

Raymond Atuguba, Moritz Hennemann,
Patricia Boshe, Sena Dei-Tutu

https://doi.org/10.1515/9783110797909-001

Table of Contents

List of Abbreviations

ACHPR	African Charter on Human and Peoples Rights
ADR	Alternative Dispute Resolution
AEPD	Agencia Española de Protección de Datos
AEPD	Agencia Española de Protección de Datos
AfCFTA	The Africa Continental Free Trade Agreement
AI	Artificial Intelligence
Art	Article
ATIP	Access to Information and Privacy (ATIP)
AU	African Union
AUDA-NEPAD	Africa Union Development Agency-New Partnership for Africa's Development
CBK	Central Bank of Kenya
CERT	Computer Emergency Response Team
Cap	Chapter
CIPESA	Collaboration on International ICT Policy for East and Southern Africa
CNIL	Commission Nationale de l'Informatique et des Libertés
CoE	Council of Europe
COVID-19	Coronavirus disease – 19
DDPL	Domestic Data Protection Law
DMS	Device Management System
DNA	Deoxyribonucleic Acid
DPA	Data Protetcon Authority
DPD	Data Protection Directive
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DTS	Digital Transformation Strategy
EAC	East African Community
EC	European Commission
ECCAS	Economic Community of Central African States
ECHR	European Convention on Human Rights
ECOWAS	Economic Community of West African States
EDPB	European Data Protection Board
eIDAS	electronic Identification, Authentication and Trust Services
eKLR	Electronic Kenya Law Reports
EU	European Union
GCI	Global Cybersecurity Index
GDP	Gross Domestic Product
GDPR	General Data Protection Regulations
GPS	Global Positioning System,
GSMA	Global System Mobile Association
ICCPR	International Covenant on Civil and Political Rights
ICO	Information Commissioner's Office
ICT	Information and Communication Technology

https://doi.org/10.1515/9783110797909-002

ICT4AD	ICT Policy for Accelerated Development
ID4D	Identity for Development Initiative
ISO	International Organization for Standardization
ISP	Internet Service Providers
ITU	International Telecommunications Union
KDPA	Kenya Data Protection Act 2019
KLR	Kenya Law Reports
NADPA	Network of African Data Protection Authorities
NCC	Nigerian Communication Commission
NCSA	National Cybersecurity Authority
NCSC	National Cyber Security Centre
NDPA	Nigeria Data Protection Act 2023
NDPR	Nigerian Data Protection Regulations
NGOs	Non-Governmental Organizations
NIMC	Nigerian National Information Management Commission
NIN	National Identification Number
NIST	National Institute of Standards and Technology
NITDA	National Information Technology Development Agency
NTP	National Telecommunication Policy
ODPC	Office of the Data Protection Commissioner
OECD	Organisation for Economic Co-operation and Development
OTTs	Over The Top Services
P	Page
Para	Paragraph
PIA	Privacy Impact Assessment
POPIA	Protection of Personal Information Act
POTRAZ	Postal and Telecommunications Regulatory Authority of Zimbabwe
PRIDA	Policy and Regulation Initiative for Digital Africa
RDPL	Rwanda Data Protection Law
Reg	Regulations
RFID	Radio Frequency Identification
RICA	Regulation of Interception of Communications Act
SADC	Southern African Development Community
SALRC	South African Law Reform Commission
SDG	(United Nations) Sustainable Development Goals
SIM	Subscriber Identity Module
UN	United Nations
UNDHR	Universal Declaration of Human Rights
UNICEF	United Nations Children's Fund
V	Versus

Part I **Data Protection Architecture**

Patricia Boshe

An Introduction – Data Governance in Africa: A Change in Narrative

A African Union: Pre-2020 Era

For a long time, Africa as a region has been viewed as a slow progressor in data protection and digital governance.[1] On the one hand, legal developments and reforms by African Union (AU) members were not only slow[2], but also transplants of foreign legal frameworks[3], and on the other hand, the AU seemed to have lacked leadership in related legislative initiative[4]. The AU took the first legislative step in 2014, by adopting the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). This is nineteen years after its counterpart – the European Union (EU) – adopted the first regional comprehensive data protection framework – the Data Protection Directive (1995 Directive)[5]. It took an additional nine years for the Malabo Convention to become operational.[6] This was in

1 AA Lukman, 'Giving 'Teeth' to the African Union Towards Advancing Compliance with Data Privacy Norms' (2021) 30 *Information & Communications Technology Law* 87 at 101.
2 See further on Chapter four, 'Tech Law as Politics in Africa' by Mailyn Fidler.
3 P Boshe, MS Hennemann, & R von Meding, 'African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward' (2022) 3 *Global Privacy Law Review* 56 at 57, 60–61. Cf. AA Lukman, 'Giving 'Teeth' to the African Union Towards Advancing Compliance with Data Privacy Norms' (2021) 30 *Information & Communications Technology Law* 87 at 100.
4 Ibid, p. 88.
5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.
6 Alt Advisory, 'Africa: AU's Malabo Convention set to enter force after nine years' *Advisory Notes, Data Privacy*, https://altadvisory.africa/2023/05/19/malabo-convention-set-to-enter-force/ accessed on 16.11.2023.

https://doi.org/10.1515/9783110797909-003

June 2023, after it attained the 15th ratification from an AU member (Mauritania) – 15 ratifications as required by Article 36 Malabo Convention to come into force.[7]

For purposes of clarity, and for international readers who may not be familiar with the AU legislative approach, some background information might be helpful. The AU is an intergovernmental organization, different from, for example, the EU which is a supranational organization.[8] As a result the AU lacks "power over state parties to compel compliance with their international/regional obligations as the EU does."[9] Consequently, the AU cannot enact or adopt a self-executing legal instrument as the EU did with the General Data Protection Regulation (GDPR) in 2016. In the same realm, the AU "cannot compel member states to sign or ratify treaties."[10] Ratification of treaties is 'solely' dependent on the political will of a member state. This is also compounded by the architecture of the Malabo Convention. The latter failed to give the AU the power to sanction member states for non-compliance. As such, the AU had a limited role in ensuring that the Malabo Convention attains the required 15 ratification without delay.

The Malabo Convention creates a unique framework. It establishes not just a data protection framework, but also frameworks for "Cyber Security and Combating Cybercrime" and "Electronic Transactions". This architecture speaks of the AU's vision in regulating digital economy. A vision fitting for the digital economy and uniquely 'invented' by the AU. In the words of Ayalew, the Convention "offers a holistic continent-wide framework to harmonize [...] digital rights".[11] This is confirmed later in 2022, in the African Union Data Policy Framework (DPF) to which we will return to later.

B African Union: 2020 and Beyond

The seemingly AU's lack of leadership took a turn in the beginning of the year 2020. In its effort to build a secured and reliable information society, the AU invested in

7 Article 36 states, "This Convention shall enter into force thirty (30) days after the date of the receipt by the Chairperson of the Commission of the African Union of the fifteenth (15th) instrument of ratification."

8 Lukman (n. 1), p. 89.

9 Ibid.

10 Ibid.

11 YE Ayalwe, 'The African Union's MalaboConvention on Cyber Security and Personal Data Protection enters Force: What does it mean for Data Privacy in Africa of Beyond? EJIL:Talk, https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/ accessed on 16.11.2023.

collaboration, international partnerships and assistance. A strategic move that allowed the AU to learn as well as to gain capacity and relevant skills to build the necessary governance structures. The Policy and Regulation Initiative for Digital Africa (PRIDA) is one notable initiative.[12] Although PRIDA initiative started in 2017, results started showing around the year 2020. Beyond PRIDA, the EU pledged to continue supporting Africa digital revolution. Although the EU took this as an opportunity to continue promoting its values[13], Africa took it as an opportunity to lead the digital economy[14] and "promote Africa's position in the world's digital economy"[15].

The EU's pledge to support Africa manifested into different projects. Notable are the EU-AU Digital Economy Task Force (EU-AU DETF)[16] and the AU-EU Digital4-Development Hub (D4D Hub)[17]. While the PRIDA project started in 2017, the EU-AU DETF was established in 2018 and the D4D Hub was launched in 2020.[18] Technical assistance to the PRIDA project ended its task in 2023. During the project period, African Union Commission (AUC) developed numerous digital strategies and programs. These include the Digital Education Strategy, Digital Health Strategy, Digital Agriculture Strategy, Strategy on Policy and Regulation Harmonization to support the Digital Single Market. It performed a detailed study on Artificial Intelligence (AI) in Africa, established a methodology and measured the level of harmonization of data protection in the region, developed a methodology and measured the level of harmonization of license for mobile operators, launched the School of Internet Governance and Internet Governance Fora (IGF), and developed online trainings (Internet Governance Courses) for diplomats and general audiences.

Within one year of its establishment, the DETF came up with a report and recommendation to support AU's dream to create an African digital single market.[19]

---

12 PRIDA is a joint initiative between AU, EU and the International Telecommunication Union (ITU). It was geared to support Africa through digitalization. This initiative went beyond governance (policy, regulatory and legislative support) to include support in building digital infrastructure and 'connect' Africa to the world to participate in global internet governance dialogues. See https://prida.africa/about-us/ accessed on 16.11.2023.

13 European Strategy for Data (European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European Strategy for Data*, COM (2020) 66 final), p. 24.

14 AU, *The Digital Transformation Strategy for Africa* (2020–2030) at p. 3.

15 Ibid., at p. 37. Cf. Boshe, Hennemann, & von Meding, (n. 1) at 82.

16 More information about the initiative https://ec.europa.eu/futurium/en/eu-au-digital-economy-task-force.html accessed on 16.11.2023.

17 Information about the initiative can be found https://d4dhub.eu/ssa accessed on 16.11.2023.

18 Cf. Boshe, Hennemann, & von Meding, (n.1) at 84.

19 Boshe, Hennemann, & von Meding, (n.1) at 84.

In addition, it is this very Task Force that recommended to the AUC to adopt the Digital Transformation Strategy. The latter (Digital Transformation Strategy for Africa (2020–2030) (DTS)) was adopted in February 2020, a year after the DETF recommendation.[20]

The DTS set the pace to the AU leadership in data and digital governance. One of the major regulatory moves by the AU, following the DTS is the DPF. The DPF was adopted two years after the DTS, i.e in 2022. Like the Malabo Convention, the DPF insists on a holistic data protection and digital governance approach. In the words of Amani Abou-Zeid, AU Commissioner for Infrastructure and Energy:

> a. "[t]he AU Data Policy Framework [is a] significant step toward creating a consolidated data environment and harmonised digital data governance systems to enable the free and secure flow of data across the continent while safeguarding human rights, upholding security and ensuring equitable access and sharing of benefits..... Through this framework, African countries agree to put in place the needed mechanisms and regulations to cooperatively enable data to flow across Africa and pave the way to the achievement of the Digital Single Market [...] and thrive in the global digital economy and society."[21]

There are many novel governance and regulatory aspects introduced by the DPF. One of the recommendations propose the establishment of a data categorization framework.[22] The DPF envisions the categorization of data beyond the conventional 'personal' and 'non-personal data'. It might extend to aspects such as proprietary data.[23] Indeed, in June 2022, the AU advertised a tender for the "Consultancy Services to Develop Data Categorization and Sharing Framework that takes into account the broad types of data and the associated levels of privacy and security".[24] Unfortunately, the AU has neither published the winner of the tender nor the status in developing the framework so far.

The DPF also insists on the provision of guidelines to promote data value creation[25] and open access to data to support local innovation and entrepreneurship. The two latter aspects cements on the approach set by the Malabo Convention. In its Art. 8, the Convention insists that data protection should give primary consid-

20 Boshe, Hennemann, & von Meding, (n.1) at 81.

21 The AU Data Policy Framework was endorsed by the Executive Council during its 40th Ordinary Session held on 2–3 February 2022 through Decision with reference http://ex.cl/Dec.1144(XL), Addis Ababa, at p. iv.

22 Ibid., pp. vii, x, 48, 52 and 59.

23 Ibid., pp. vii, 23, 24 and 59.

24 The advertisement is accessible at the AU website, https://au.int/en/bids/20220615/consultancy-services-develop-data-categorization-and-sharing-framework-takes-account accessed on 17.11.2023.

25 Ibid., pp. 5, 7, 25, and 37–39.

eration to state prerogative, the rights of local communities and business purposes. This demonstrates that, despite being considered as a late comer and slow in legislation, the AU approach to digital governance is meticulously planned and well calculated to accomplish the final goal, i. e. the creation of the African Digital Single Market. And although AU and its member states had been seen as 'copying' other governance frameworks, the continent has its distinct approach to data and digital regulation. An approach that needs a careful eye, an understanding, and an assessment of all-encompassing regulatory actions to understand its direction.

The DPF recommendation for transversal collaboration between data related regulatory bodies is also worth mentioning.[26] The DPF proposes a "collaboration between regulatory institutions across different mandates and coordinated market regulation (in interrelated policy areas such as telecommunications, finance, competition, trade, taxation and data regulation)."[27] In 2020, Ademuyiwa and Adeniran foretold this of Africa. They foresaw an "opportunity for African policy makers to do things differently with the newly emerging digital markets, and to learn from the mistakes of the front-runners (advanced economies)."[28] They saw Africa as a potential forerunner in designing a data regulatory merger system more fitting for the digital economy. A system that is "more pragmatic, relying heavily on cross-country harmonization, cooperation and collaborations."[29] Their advice encompasses a data governance structure that consists of a complementary legal, regulatory and policy framework. As an example, they point out "competition laws, [...] digital sector taxation, consumer protection laws, data protection and privacy laws, cross-border data flows and data localization measures, and digital entrepreneurship and digital skills development programs"[30] as aspects that should neither be developed nor regulated in isolation. Indeed, the DPF takes this approach to data governance.

Unlike other data (protection) governance systems, the DPF is intended to support data related innovation, not to restrict them. The underlying mission of this governance structure is to create value in data to support data entrepreneurship while safeguarding human rights. For example, it insists, on the one hand, in stimulating "demand for data, which includes incentivising innovative data communities, and, on the supply-side, ensuring the quality, interoperability, and relevance

26 The AU Data Policy Framework (n. 21), p. 40.

27 Ibid., p. 44.

28 I Ademuyiwa & A Adeniran, 'Assessing Digitalization and Data Governance Issues in Africa' CIGI Papers No. 244 – July 2020, *Centre for International Governance Innovation*, p. 9.

29 Ibid.

30 Ibid., p. 10.

of data in both the public and private sectors and civil society"[31]. On the other hand, to "promote interoperability, data sharing, and responsiveness to data demand through the setting of open data standards in data creation that conform to the general principles of anonymity, privacy, security and any sector-specific data considerations to facilitate non-personal data, and certain categories of personal data are accessible to African researchers, innovators and entrepreneurs."[32]

The DPF is a policy innovation. The policy innovation that signals the AU's shift from a dormant to an innovative and forward-thinking policy maker.

Not to forget, in the same year, in June 2022, the AU made another significant regulatory move. This was the review of the Malabo Convention. The AU published a consultancy call for the review of the Malabo Convention.[33] Sadly, just like the consultancy call for data categorization mentioned above, the AU has neither communicated (publicly) the winner of the tender nor the status of the review.

C Africa(n Union) to the World

At the global level, the AU seems to assert its position more strongly than before. An example is the US-Africa summit of 2022. In asserting its position as an equal player in global decision making, "senior U.S. government officials displayed remarkable openness to listening to, and collaborating with their African counterparts"[34] says Zainabu Usman and her colleagues. This overcame the long-standing US attitude about inadequacy of African institutions. An attitude that led the US "to delegate lower-ranking American officials to engage with senior African policymakers."[35] Going back to the DPF, this marks an accomplishment of one of the policy recommendations, i. e. that Africa should demand a sit at the table in global

31 Ibid., p. viii.

32 Ibid.

33 The tender was initially advertised here. https://au.int/sites/default/files/bids/41922-RE-ADVERTISEMENT_-TOR_Legal_Expert_Malabo_Convention_on_Cybersecurity_an.pdf Unfortunately, the webpage is no longer accessible. However, here is the information about the tender. 'Consultancy Services To Review The Malabo Convention On Cybersecurity And Personal Data Protection And Recommend Possible Amendments To Articles.' The tender was released on Jun 18, 2022. GT reference number – 474453100 Product classification – 72206200.

34 Z Usman, J Ovadia & A Abayo, 'The U.S.-Africa Leaders Summit Marks a Seismic Shift in Relations with the Continent' (December 2022) Commentary, https://carnegieendowment.org/2022/12/22/u.s.-africa-leaders-summit-marks-seismic-shift-in-relations-with-continent-pub-88692 accessed on 16.11.2023.

35 Ibid.

policy-making fora rather than continue being "standard takers" in global governance.[36]

The AU assertiveness prompt the launch of the Digital Transformation with Africa (DTA) initiative. An initiative between Africa and the US that aims to support Africa's digital transformation, including the implementation of the DTS[37] and the AfCFTA[38]. This also led President Biden recommending the inclusion of the AU as a permanent member of the G20 (now G21). A recommendation which was implemented a year later (in September 2023).[39] As a permanent member of the G21, AU has now a sit at the table and an opportunity be an active participant in the reform of global governance frameworks.

D African Union Data / Digital Economy Governance: Coming Up

The AU accomplished the aforementioned steps despite its lack of a direct mandate to regulate its member states. This also indicates the potential for the AU to go much further given proper coordination and collaboration with its member states. In November 2023, the AU organised the very first Data Governance and Innovation Forum for Africa (DGIFA) at its headquarters in Addis Ababa, Ethiopia, followed by the 5th Ordinary Session of the Specialized Technical Committee on Communication and Information Communications Technology[40]. The latter's agenda includes strategizing the implementation of the DPF. Other aspects on the agenda included the implementation of the AU Interoperability Framework for Digital ID, Draft Continental Strategy on Policy and Regulatory Environment for Africa's Dig-

36 The AU Data Policy Framework (n. 21)., p. VII, 2 and 17.

37 DTA intends to invest over $350 million and facilitate over $450 million in financing for Africa in line with the African Union's Digital Transformation Strategy and the U.S. Strategy Toward Sub-Saharan Africa. See The White House, 'FACT SHEET: New Initiative on Digital Transformation with Africa (DTA)' at https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/14/fact-sheet-new-initiative-on-digital-transformation-with-africa-dta/ accessed on 16.11.2023.

38 https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/statement-ambassador-katherine-tai-signing-memorandum-understanding-cooperation-trade-and-investment

39 World Economic Forum, 'The African Union has been made a permanent member of the G20 – what does it mean for the continent?' https://www.weforum.org/agenda/2023/09/african-union-g20-world-leaders/ accessed on 16.11.2023.

40 AUC 5th Ordinary Session of the Specialized Technical Committee on Communication and Information Communications Technology – 'Accelerating digital transformation and advancing communication and advocacy in Africa.' (November 20–24 2023) Addis Ababa, Ethiopia, https://au.int/en/5thstccict accessed on 16.11.2023.

ital Single Market, Draft Conceptual Framework of the Continental Strategy on Artificial Intelligence (AI), Cybersecurity Landscape in Africa: Assessment of Gaps and Priorities Report, Draft Child Online Safety and Empowerment Policy, Digital Transformation Strategy: Sectorial Digital Strategies (Education, Agriculture and Health), African Union Digital Health Strategy, African Union Digital Education Strategy and Implementation Plan, Improving the Digitalization of Postal Services in Africa, Acceleration of Programme for Infrastructure Development in Africa ICT projects, enhancing communication, advocacy and understanding of the African Union Agenda, and Data Governance & Innovation Forum for Africa.

In short, the year 2022 saw AU's major paradigm shift not only in policy and governance approaches, but also in asserting its global position in the (digital) global economy as well as in the international order. In fact, this shift seems to frighten some of the global regulatory leaders. Shiferaw and Di Ciommo argue that the AUs "assertiveness and increasing global importance alongside Europe's declining centrality in the global economy and politics, as well as the emergence of a multipolar world"[41] negatively impacts AU-EU partnership. They highlight the "credibility of the current Western-led global governance system" leading to African countries to "not only demand more representation but also push back against the unidirectional ways of norms enforcement that underlie the partnership, [among other reasons] the policy divergences and mistrust among policymakers on the two continents have increased in recent years."[42]

E Conclusion

Against these manifold backgrounds, in 2022, the first major continental-wide conference on *African Data Protection Laws: Regulation, Practice, and Policy* took place. The conference was organized by the University of Ghana School (UGSoL) of Law and the Research Centre for Law and Digitalisation (FREDI) of the University of Passau, Germany. The three days-conference took place at the UGSoL and brought together data (protection) governance professionals, scholars, members of the academia and practitioners from across the globe. It spotlighted the developments of data (protection) laws in Africa and opened a platform to discuss not only data protection laws and policies but also data-related issues emerging in Af-

41 LT Shiferaw and M Di Ciommo, 'Trouble in paradise: The EU-Africa partnership in a geopolitical context' ECDPM Brief 13 November 2023, https://ecdpm.org/work/trouble-paradise-eu-africa-partnership-geopolitical-context accessed on 16.11.2023.

42 Ibid.

rica, specifically data governance, data localization and the digital economy, with a pan-African perspective.

This volume builds upon earlier publication[43] and comprises of papers presented during the 2022 conference. The volume encompasses next to Part I (Introduction and General Setting) Part II on African Approaches and Data Colonialism, Part III on Law Enforcement and Part IV on Re-Imagining the Future.

Part I sets the motion with this very introductory chapter as well as with the chapter by Peter Kimpian on 'Rights to Privacy and to Personal Data Protection and Convention 108'. Kimpian explains the role of international organizations in the development of legal standards. Speaking from the perspective of the Convention 108[44], Kimpian describes how this Convention helped to harmonise data protection standards beyond Europe. He explains that Convention 108, being the first and the only binding international instrument on data protection, has helped to form a foundation to many data protection frameworks in Europe and beyond. He argues that the fact that the Convention is open to members beyond Europe made it possible for countries beyond Europe, including in Africa to ratify and built up their local regulatory frameworks. Kimpian further asserts that, being the first international regulatory framework, this Convention's practical rules fit the ever-evolving digital economy. According to Kimpian, the Convention has not only been tested for a longer time, but also occassionally reviewed to address new and emerging risks associated with digital economy.

According to Kimpian, some AU member states have benefited from this principle-based, flexible framework for the protection of individuals' privacy and personal data. He argues that the Convention framework supports and provides viable forum for cooperation to supervisory authorities. Through this, it has managed to provide support to emerging and growing states, including in Africa, to develop and review their legal frameworks to meet international accepted standards. He mentioned some of the African states that received such support to include Mauritius, Senegal, Tunisia, Capo Verde and Morocco. On this chapter, Kimpian raised his approval of the standards established by the Malabo Convention "whose data protection framework and values reflects, in principle, those promoted by the CoE 108 but tailored to fit African countries". He also indicated Council of Europe's support to "Network of African Data Protection Authorities ("NADPA") in their effort to create a truly African network for cooperation, for knowledge and best-practice sharing, for joint actions and for international cooperation, rep-

43 MS Hennemann (ed), *Global Data Strategies*, 2023.

44 Convention 108 for the protection of individuals with regard to automatic processing of personal data (ETS No. 108, January 28, 1981) and its additional protocols.

resentation". He concludes by assuring the never-ending support and cooperation to countries in Africa and the AU in legal and policy development in the area of data protection.

The second part starts with a chapter by Lukman Abdulrauf on 'African Approach(es) to Data Protection Law'. He examines the existing debate on whether there is a unique African understanding of data protection law and enforcement mechanisms that are traditionally 'African'. An approach that resonates with African cultural norms and traditional approach(es) to dispute resolution. Abdulrauf's chapter intends to respond to questions and debates that emerged due to African countries transposing foreign legal norms, especially the GDPR. Some of which questioned the suitability of foreign legal norms in an African context, and others which demand for decolonisation, Africanisation, and African solutions to African problems approach to law-making.

To answer these questions, Abdulrauf focuses on the 'contents of *sui generis* data protection laws. He looks into the data protection policy-making approaches and reasons. He found lack of an overarching concern that has led to the adoption of data protection laws specific to 'all' of Africa. However, he identified a common factor to be the pressure to satisfy the EU 'adequacy' requirement introduced by Article 25 of the EU Directive for trade purposes. It is also pointed to the fact that most African countries received financial and technical support from European bodies in the making of their data protection laws. He further argues that, even for African countries that incorporated data protection guarantees in their constitutions (separate from the right to privacy), such frameworks still echo thick European roots. Of course, this confirms neither the presence nor the absence of 'African approach' to data protection. It only speaks of legislative approach taken by most African states including the AU.

To elucidate on the 'African approach', Abdulrauf comments on the ubuntu philosophy. A philosophy believed to speak of an African value. He argues that Ubuntu's underlying principle, human dignity, is not a special 'African' principle. In fact, this is the very principle that builds European data protection framework. He further points to other aspects such as the protection of community rights and the rights of vulnerable groups under the Malabo Convention, the inclusion of Alternative Dispute Resolution (ADR) in the Kenya Data Protection Framework. Aspects that are often perceived as speaking of a unique African value. But he concluded that 'these are merely isolated features and are rarely common to data protection laws in Africa'.

Abdulrauf considers a search for an 'African approach' as a futile exercise, at least in the sphere of data protection. First, because African legal systems are pluralistic systems which have further been complicated by colonial history that created patches such as common law and civil law systems. As such, no one legal cul-

ture or African value can be foreseen. Second, data protection laws are centred on principles and core values that are similar across the world. He believes, instead of clinging on establishing 'African approach' (whose existence cannot be proven and which lacks a well-defined agenda), we should think in terms of the Africanisation of data protection laws. A concept which he elaborates as involving a process of consciously promoting indigenous thinking and knowledge in various facets [leading to] thinking in terms of 'African solutions to African problems. An approach that he believes will also bring light to the digital / data imperialism (data colonialism) debate. The chapter therefore forms a starting point to get the intricacies of this narration, to understand the 'African privacy' debate and to value anti-colonial approaches.

A further continuation of the Africanisation in law is presented by Mailyn Fider in her chapter titled 'African Data Protection Laws: Politics, But as Usual'. Fidler underlines the existence of an African solution to African problems cybersecurity regulation in Africa. On the contrary, she notes that, with data protection, African states do not seem to pursue African solutions to African problems approach to law-making. Fidler investigates how political will and political power (both within Africa and beyond) influences law-making process and the law itself (the product) in Africa.

Fidler believes that economic threat brought about by Art. 25 1995 Directive and Art. 45 GDPR gave African countries no choice but to comply. The compliance meant African countries enacting similar data protection frameworks as that of the EU – to underline their wish to maintain access to European markets. To the contrary, no such consequences exist in the area of cyber security regulation (i.e the Budapest Convention). As a result, African countries are 'free' to design their frameworks to suit their local problems and to provide for African solutions. Fidler argues that external powers can take away law-making autonomy from African countries. She uses an example of EU data protection framework and the adoption of the European-style data protection frameworks in Africa to illustrate this. The chapter uses legislative trends in both Africa and Europe to narrate how power and politics influence law-making.

Part III focuses on data protection enforcement on the African continent. The starting point is a chapter by Iheanyi Nwanko and Nelson Okeyo on 'Adopting Data Protection Impact Assessment (DPIA) in Africa: Lessons from Kenya's DPIA Framework and Experiences.' The instrument of DPIA is a risk-orientated approach adopted by several countries in their data protection frameworks. The chapter demonstrates the historical development of this approach. A history that narrates its importance in the protection of privacy and later, personal data. The chapter also explains what, when and how DPIA are to be conducted. Nwanko and Okeyo also illustrate how DPIA had been implemented in various European coun-

tries and how it helped to mitigate and prevent risks to individual privacy and secure the protection of personal data.

Unfortunately, the approach has not been widely adopted at the regional and sub-regional levels. At national levels, however, countries are adopting the DPIA instrument. In some countries it is an obligation and some recommend it impliedly. The authors provide a table of 24 (out of 54) African states whose data protection frameworks provide for an obligation (expressly or impliedly) to conduct DPIA. One thing to note from this chapter is the fact that neither the adoption nor the implementation of DPIA is uniform in African countries. For this reason, the authors selected Kenya as their focal point of discussion. The fact that Kenya is probably the only country so far in Africa having not only a DPIA in the law but also have it litigated in the highest Court made it a suitable candidate for this assessment.

Speaking of Kenya's experience, the authors believe that proper implementation of the DPIA needs not only an independent commission, but also a competent one. In this case, they argue that the Kenya Office of the Data Protection Commissioner (ODPC) is both. This office has managed to publish a Guidance Note and a template for conducting DPIA. Furthermore, the ODPC scrutinizes DPIA reports. According to the authors, this is an important aspect least DPIA will turn into a mere box-ticking exercise.

The authors point to the fact that the ODPC has been proactive. For example, the ODPC published a list of processing activities that DPIA is mandatory, the so called blacklist for DPIA. This is to ease data protection controller in ascertaining when to conduct DPIA. They also attribute to the growth of self-regulation and sector-specific regulations in Kenya. Both of which are an inspiration of a risk-based approach to data protection – and the very essence of DPIA. Thereby, the chapter provides not just an extensive understanding and importance of DPIA in protecting personal data, but also an exposé on its practical implementation, especially in the African context.

Nwanko and Okeyo also indicate that Ghana lacks an express provision for DPIA. This requirement is only implied as part of security measures imposed on data controllers and processors. On the succeeding chapter Setor Foe-Ahorney raises the question 'Does the law protect the privacy of Ghanaians on the internet?'. In this exploratory study Foe-Ahorney assesses the sufficiency of legal framework (beyond data protection) in protecting Ghanaian on the internet. Her study is prompt by increasing number of online incidents (cybercrime and cybersecurity incidents). She gives the extent of the problem by referring a study by the FBI ranking Ghana as second of the cybercrime-offending countries in Africa (after Nigeria). She questions how, despite a fleet of laws (such as cybersecurity Act, Data Pro-

tection Act, Electronic Communications Act), Ghanaians are still very vulnerable online and unable to get protection online.

In the end, Foe-Ahorney comes to the conclusion that the problem does not lie in the 'adequacy' of the law / legal framework, but rather in the actual implementation of these laws. She also notes that some laws pre-date the internet, making it hard to prosecute online crimes. She also points to other reasons which are typical in many African countries – and potentially even beyond Africa.

Ridwan Olodeye's and Aishat Salami's chapter then examines 'Digital Identity, Surveillance, and Data Protection.' The authors explain the inevitability of digital identity in the digital economy era – in particular to support social inclusion and civil participation. They also presented the down-sides of digital identity. The authors present an outlook in rolling-out digital identity systems. A process involving the collection of personal data by governments. Not just 'simple' personal data, but also sensitive personal data such as biometric data (finger prints, iris) and facial features. A process tied to the creation of large databases with personal data. According to the authors, this fact has simplified or facilitated surveillance of citizens for purposes beyond individual identification. They point to the example of Nigeria where the government has been using digital identity database to monitor and silences dissidents and critics. Elaborating further on the Nigerian context, the authors argue that the existence of more than ten different state and federal government agencies establishing biometric identity systems and maintain their distinct systems further support illegitimate surveillance of individuals by linking different activities they do from different agencies. The most frightening aspect advanced by the authors is the fact that digital identity systems in most African countries are linked to individual's SIM card registration which is (often) mandatory in those countries.

Throughout this chapter, one is put into a position to visualize how individual life can be scrutinized from just data collected through digital identity roll-out. From financial transactions (through mobile money), communications, location (attached to communication towers) and beyond. Unfortunately, the authors do not show much confidence in data protection laws / frameworks of most African countries to address the nature of data processing involved in digital identity systems. Not just in the context of digital identity systems, the implementation of data protection laws, in general, in Africa is still problematic. This chapter gives a glimpse of the horror of digital identity systems on the privacy and personal data protection on the continent.

Nevertheless, digital identity remains an important aspect in the digital economy. An important consideration for African countries is to strengthen security measures in the deployment of digital identities and set up a transparent and oversight mechanism to mitigate potential abuse. This takes us to the next chapter by

Victoria Oloni titled 'Cross-Border Data Flows: Oiling the wheel of the African Digital Economy.' Oloni examines the role of cross-border free flow of data in building digital economy in light of the growing data localization regulations in Africa. She starts by explaining different (regulatory) approaches to cross-border data flows and shows that these approaches have been codified in specific data protection laws in some African countries. She then turns to the position of the AU and refers to the DPF. According to Oloni, the DPF suggests to countries to carefully consider human rights when adopting data localization regulations. In addition, the DFP insists on an equilibrium between advancing balanced economic growth and ensuring sufficient data security in the design of cross-border data flow rules and suggests cross-border collaboration to support this.

In further examining the Malabo Convention, the Personal Data Protection Guidelines for Africa 2018 and the DTS, Oloni shows differing approaches suggested by these instruments, but notes an alignment in one aspect, in relation to cooperation and collaboration by data protection authorities on the continent. Ideally, this is considered as a way to ensure interoperability and security of personal data across borders. She notes, however, that data localization poses a threat to cross-border free flow of data and eventually, impend on the growth of digital economy. She considers justifications advanced for data localization regulation to be valid. Nevertheless, she believes there is a better way to address those concerns rather than to adopt data localization regulation.

The discussion of data localization measures is continued by Melody Musoni. She looks at the 'Role of Data Localisation in Cybercrime Investigations'. Musoni starts by explaining concerns that lead to the sprouting of data localization regulation in Africa. One of the reasons she advanced is the lack of data centre capacity in Africa which results in African data being hosted on data centres located abroad. A fact that she considers to affect criminal investigations when law enforcement needs to access data stored in a foreign jurisdiction. According to her, data localization comes in as a solution to ensure timeous evidence gathering and successful prosecution of crimes. She also brings in counter arguments against data localization, such as enticing cybercrimes and external surveillance.

Musoni explains in depth the matrix around accessing data in a foreign data cloud and why it makes it difficult for law enforcement (in Africa) to discharge their duties. She also explains the dangers of having all data located locally in a single place.

This volume concludes with part four taking us to 'Re-Imagining the Future'. Brian Tshuma elaborates on 'Data Imaginaries and the Emergence of Data Institutions in sub-Saharan Africa'. Tshuma makes a call to re-think data-related legislative approaches in Africa. He starts by going through the discussions on emerging technology and inappropriateness of foreign imposed legal frameworks on Africa's

diverse data communities. Tshuma argues that, with emerging algorithmic technologies reducing governance to the management of atomistic behaviors', it is futile to have a foreign framework to govern the sphere. He proposes a change by calling the reader to re-imagine datafication process (in Africa) with data as a public good that belongs to the people. He advances the idea of data imaginaries as a starting point to this end. Data imaginaries entail the way to imagine data and its existence which is not 'divorced' from norms, expectations, social processes, transformations and social ordering. By doing so, African societies are called to re-imagine regulatory frameworks that align with African data imaginaries. Through this approach, new, collective governance models, and an alternative set of concepts and values to steer the new envisioned governance' can be created.

Brian Tschuma pleads together with African scholars, policy makers, practitioners to imagine a data governance framework independent from the GDPR-type regulatory approaches. Preferably, a governance framework that creates a space for data community to be heard and 'interplay of norms, rather than simply the regulation of data through policy and law.' Tshuma calls for African countries to think outside the box and consider the interplay between and within different data communities and data categories and everyday life activities involving the use of data.

F Bibliography

Ademuyiwa/Adeniran, 'Assessing Digitalization and Data Governance Issues in Africa' CIGI Papers No. 244 – July 2020, *Centre for International Governance Innovation.*

Alt Advisory, 'Africa: AU's Malabo Convention set to enter force after nine years' *Advisory Notes*, *Data Privacy*, https://altadvisory.africa/2023/05/19/malabo-convention-set-to-enter-force/ accessed on 16.11.2023.

AUC, AU Data Policy Framework was endorsed by the Executive Council during its 40th Ordinary Session held on 2–3 February 2022 through Decision with reference http://ex.cl/Dec.1144(XL), Addis Ababa

AUC, *The Digital Transformation Strategy for Africa* (2020–2030).

Ayalwe, 'The African Union's MalaboConvention on Cyber Security and Personal Data Protection enters Force: What does it mean for Data Privacy in Africa of Beyond? EJIL:Talk, https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/ accessed on 16.11.2023.

Boshe/Hennemann/von Meding, R., 'African Data Protection Laws: Current Regulatory Approaches, Policy Initiatives, and the Way Forward' (2022) 3 *Global Privacy Law Review* 56.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995.

European Strategy for Data (European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *A European Strategy for Data*, COM (2020) 66 final).

Lukman, 'Giving 'Teeth' to the African Union Towards Advancing Compliance with Data Privacy Norms' (2021) 30 *Information & Communications Technology Law* 87.

Shiferaw/Di Ciommo, 'Trouble in paradise: The EU-Africa partnership in a geopolitical context' ECDPM Brief 13 November 2023, https://ecdpm.org/work/trouble-paradise-eu-africa-partnership-geopolitical-context accessed on 16.11.2023.

Usman/Ovadia/Abayo, 'The U.S.-Africa Leaders Summit Marks a Seismic Shift in Relations with the Continent' (December 2022) Commentary, https://carnegieendowment.org/2022/12/22/u.s.-africa-leaders-summit-marks-seismic-shift-in-relations-with-continent-pub-88692 accessed on 16.11.2023.

World Economic Forum, 'The African Union has been made a permanent member of the G20 – what does it mean for the continent?' https://www.weforum.org/agenda/2023/09/african-union-g20-world-leaders/ accessed on 16.11.2023.

Peter Kimpian

Rights to Privacy and to Personal Data Protection and Convention 108

A Introduction: Council of Europe and the Right to Data Privacy

The Council of Europe[1], is a leading international human rights organisation. It was created after the 2nd World War to uphold human rights, democracy and the rule of law initially on the European continent. It has 46 member states that are all bound by its core instrument – the European Convention on Human Rights ("ECHR"). The ECHR is the first practical implementation of the Universal Declaration of Human Rights ("UNDHR"). The ECHR provides a list of individual universal human rights that all countries need to respect at all times. It is complemented with more than 250 conventions. Human rights under the ECHR are enforced through the European Court of Human Rights ("the Court"). On the one hand, the ECHR, set major standards for its member states, on which modern democracies are being based, and on the other hand, the Court whose decisions are binding to member states, guard human rights of more than 700 million citizens. With more than 261 cases[2] only on the right to privacy (article 8) in the last 12 months, the Court ensures the highest legal protection possible against member states' violations and unlawful interferences.

The Council of Europe is mandated to set new standards as international public law (such as recently started on artificial intelligence[3]). It also carries out, as a complement, an evaluation and follows up on activities to ensure a harmonised

1 https://www.coe.int/en/web/portal/home.

2 https://hudoc.echr.coe.int/fre/#{%22article%22:[%228%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22kpdate%22:[%222022-02-02T00:00:00.0Z%22,%222023-02-02T00:00:00.0Z%22]}.

3 https://www.coe.int/en/web/artificial-intelligence.

https://doi.org/10.1515/9783110797909-004

interpretation and a coordinated implementation of those conventions. These operations are further enriched by a wide range of cooperation activities financed by the member states and external donors, ran through cooperation programmes and specific projects to identify, and fill gaps in the implementation of those standards. Since the 1980s' some of the standards (on corruption, data protection, cybercrime, money-laundering, sport integrity, artificial intelligence etc.) have been incorporated, on purpose, in – so called – "open" conventions for that countries outside of the European continent could also adhere to them and participate in their development and implementation as well. As such, the Council of Europe is not only seen as a purely regional organisation but through these open conventions, as relevant actor in a global context as well.

In addition, Convention 108 enables states Parties to develop data protection legal frameworks that offer a level of protection of personal data that meets the highest standards and that are accepted and recognised by countries, and regional organisations.

B The Convention ETS No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data

The right to privacy is universally recognised by article 12 of the UNDHR and Article 17 of the International Covenant on Civil and Political Rights ("ICCPR"). The ECHR guarantees, in its turn, the right to private life in Article 8, which the European Court of Human Rights often interpreted as being "an enabling right": A right which could enable the free exercise and full enjoyment of other human rights and fundamental freedoms. The Court found in several judgements that this right will also remain a core factor in preserving human dignity and individuals' right to informational self-determination in the digital age.

The Convention ETS No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") was the first instrument to support and promote a harmonised and principle-based response to the protection of personal data. This was a result of concerns that emerged in the late 70s' due to the use of new data processing technologies that increased personal data vulnerability to abuse and misuse. To counteract the effect technology may have on the safety and security of data, the Council of Europe adopted Convention 108. The main objective being to enhance the protection of privacy of individuals as set forth by the ECHR, by including the protection of personal data which, if misused or abused could infringe into individual privacy rights – among other rights.

The pillar to this protection is embedded in its regulatory approach which intends to provide for a workable legal framework to: "(...) the respect for privacy and the free flow of information between peoples[4]".

Although Convention 108 was conceived by the Council of Europe, it was never meant to be a "European" convention. This can be seen in its lack of the reference thereof in its title. Since 1981, the Convention is open for accession by any country in the world 1981. To-date, it remains the only legally binding multilateral instrument on the protection of privacy and data protection. Since the Convention is open to all interested parties, it has managed, throughout the years, to acquire 55 parties and 36 observers. In addition, it has representatives and experts from all continents. It is largely a principle-based, thus flexible framework for the protection of individuals' privacy and personal data and a viable forum for cooperation to supervisory authorities. Its conventional committee with its growing membership and active observer institutions and organizations continues to offer a unique forum for discussions and deliberations on the rights to privacy and data protection contributing greatly to the convergence towards a high set of standards globally.

The Convention has recently been modernised by the amending Protocol CETS No. 223 ("Convention 108+") with the aim to ensure, upon the entry into force, hopefully in 2024 that the free flow of data is facilitated globally, including to and from the European Union "EU") and the respect for human dignity in the digital age has legal guarantees.

Based on its territorial and material scope, its new concepts (such as accountability, privacy by design, privacy by default, privacy impact assessment, etc.) and commonly acceptable provisions also in the field of public security, there is an understanding within state Parties that it can easily be applicable to all data processing involving personal data, even if carried out by new data processing techniques and technologies (such as big data analytics, artificial intelligence, machine learning, profiling, facial recognition, etc.). Convention 108+ is not greatly detailed on every instance in order to ensure flexibility and that it can be transposed into different legal systems and jurisdictions. While being flexible, it is believed that its provisions could certainly give enough reassurance to a country and to individuals covered by its jurisdiction to address personal data/privacy related concerns in relation also to the use of new data processing techniques and technologies in both public and private sector.

4 Preamble of Convention 108, https://rm.coe.int/1680078b37 accessed on 20.10.2023.

Building on the effective and efficient implementation of its provisions underpinned by new powers and functions of its conventional committee[5] and on the prospect that an increasing number of UN Member States wishes to accede to it, Convention 108+ has the envisions on becoming a global benchmark in the area of privacy and data protection. It is also because, from an EU perspective, Convention 108 has always been seen as a "*passerelle*" between EU and other parts of the world.

In an effort to support the creation of global standard, there are as much as 20 recommendations, 1 additional protocol and 1 amending protocol developed on the basis of the provision of the Convention. The latter having an impact way beyond the European continent, including in Africa. These are the result of international negotiations and agreements on often controversial regulatory contents such as profiling, the use of algorithms, and health related data, to mention just a few. In addition, there are soft law measures developed by the Committee of Convention 108 as well as cooperation programmes carried out by the Council of Europe with a considerable impact on regional, national legislation and the jurisprudence of various judicial institutions across the world.

Furthermore, there is an unprecedented potential offered by the Convention 108 in at least two areas that have just recently been started to be explored: Possibility for inter-governmental organisations to accede (having already strong connection and active participation from Interpol, OECD, EU, ICCR, IOAS etc) and to become potentially a form for cooperation and exchanges in public security related data protection matters such as the external oversight of national security agencies (as emphasised by the 5th IIOT[6]).

There are also examples where Convention 108 was used as a focal point in domestic debates to establish and ensure independence of the data protection supervisory authority (such as in Tunisia[7]). In this way, Convention 108 not only support the setting of standards but also had a positive impact on public policy, legislative and judicial work of a country (also in relation to the Argentinian national AI strategy[8]).

To acquire or keep the confidence of individuals it is becoming increasingly important to governments and economical actors that an appropriate level of protection is defined and if possible, at a global level. In recent cases where courts

5 Article 4, paragraph 3 and in Article 23, litterae e, f and h.

6 https://www.coe.int/en/web/data-protection/-/intelligence-oversight-in-the-brave-new-world-of-proportionality-5th-international-intelligence-oversight-forum-iiof-.

7 https://www.inpdp.tn/textes.xhtml.

8 https://oecd.ai/fr/dashboards/policy-initiatives/http:%2F%2Faipo.oecd.org%2F2021-data-policyInitiatives-26935.

have been invalidating international data transfer agreements, and mechanisms due to their insufficiency in protecting individual privacy and personal data, Convention 108+ can effectively contribute by providing a blueprint of a framework to ensure countries and regions maintain the flow of data in a secure manner. In return, this will secure economic relations between states and among regions. This is because of its globally accepted data protection standards.

In fact, ensuring free flow of data between its state Parties is one of its core objectives. In essence, these objective triggers inclusive growth intensified and more integrated economic, financial and businesses operations globally. A framework that addresses cross border constraints on data export. Convention 108+ framework support the digital and highly integrated, global economy. In such environment, a country, by acceding Convention 108+ can ensure that its components are part of an ideal legal framework, and overall, a business and trade friendly environment which are at the same time respectful of universally recognised human rights.

As additional benefit, states Parties to Convention 108+ commit into a mutual co-operation in order to ensure the highest level of data protection as well as a perfect compliance with international standards. Belonging to the "Convention 108+ club" means not only demonstrating a high level of data protection but also being able to rely on a strong network of peer states able to provide with assistance, advice and support. In an era of increasing digitalisation and globally identical challenges, it also means allowing competent authorities to work hand in hand. Accession to Convention 108+ would also mean a recognition of an international best practice which would open opportunities for further, enhanced cooperation, including via joint investigations and joint regulatory actions. It includes participation to the highest multilateral level in the shaping of the future of the right to data protection while contributing to maintain the free flow of data globally.

International cooperation often supposes a mutually agreeable regime on transborder data transfers. In areas such as law enforcement, financial surveillance, tax matters, humanitarian actions, security, etc. authorities of a state Party to Convention 108+ would easier interact with authorities of another or multiple state Parties, thus increasing the efficiency of their cooperation. International organisations will very likely join Convention 108+ in the future as well which would mean that the data transfer regime within the organisation and its member states will also be aligned with Convention 108+. For instance, the long debated second additional Protocol to the Budapest Convention also recognises the potential of an easier cooperation between law enforcement authorities, including the ones re-

sponsible for cybercrime and cyber security if both of them are based in a state Party to Convention 108+.[9]

C Implementing Convention 108

As the implementation of the Convention 108+ is key to its success, the Council of Europe provides expertise for state Parties and candidate countries. This is through technical assistance programmes for drafting national legislation, capacity building, empowering of institutions, and training of staff, among others. Implementation of the Convention 108 and the support from the Council of Europe also brings a potential to harmonise national practices and also provide for internationally recognised "best practices". In addition, for non-EU countries it can play an important role in obtaining and/or maintaining adequacy decisions from the EU (which means free flow of data to the EU market).

The Council of Europe, in implementing and supporting the implementation of Convention 108+ supports an important regulatory approach that provides for "a common response to collective challenges in the digital age." An approach which also is attentive to its very special relationship with the EU data protection instruments, which are recognised as golden standards in the area of the protection of personal data. These are among the main factors that were considered and supported during the negotiations to amending Protocol CETS No. 223 and most recently when elaborating guidelines in the area of data protection and new processing techniques, technologies[10].

The potential of Convention 108+ to contribute to the convergence to a set of high data protection standards was repeated and amplified via several communications from the European Commission, such as in the "Communication from the Commission to the European Parliament and the Council on Exchanging and Protecting Personal Data in a Globalised World" Section 3.3.1 (page 11) second paragraph states: "In particular, the Commission encourages accession by third countries to Council of Europe Convention 108 and its additional Protocol. [...] It is currently in the process of being revised and the Commission will actively promote the swift adoption of the modernised text with a view to the EU becoming a Party." This was also one of the messages conveyed by Didier Reynders, Commissioner for

9 https://rm.coe.int/1680a49dab, cf. Article 14.1.b ; Paragraph 222 of Explanatory Report accessed on 20.10.2023.

10 https://www.coe.int/en/web/data-protection/guidelines.

Justice, European Commission in his video message[11] delivered on the occasion of the 41st international data protection day on 28 January 2022 emphasising the Convention's importance in the process of EU adequacy decisions and its role in achieving a higher degree of regulatory convergence and a stronger corporation of supervisory authorities in the field.

It is also worth noting that the former UN Special rapporteur on the Right to Privacy has called upon all UN member countries to accede the Convention seeing its potential in converging data protection standards across the world, the first time in its 2018 Annual report presented to the UN General Assembly (2018): "As an interim minimum response to agreeing to detailed privacy rules harmonised at the global level, all UN Member States been encouraged to ratify data protection Convention 108+[…]."[12] The second time it was pronounced during 2019 Annual report presented to the UN Human Rights Council (2019).[13]All these drove Convention 108 to be the second[14] most populous convention of the Council of Europe in which the organisation and its state Parties see a strategic potential for the digital age.

Given the EU leadership and global position in digital regulation, coupled with the extra-territorial protection of EU residents' personal data through the GDPR, EU adequate protection requirements on international transfer of personal data will remain high on the agenda. Therefore, the provisions of the Convention 108 on transfer of personal data and cooperation between authorities will continue to support states beyond Europe in developing legal frameworks, and in building principles comparable or compatible with European rules.

Today, when it comes to data protection, even at international level, there is no conversation without mentioning the EU and its instruments. And very rightfully so, as the EU General Data Protection Regulation (EU) 2016/679, GDPR) and the Law Enforcement Directive (Directive (EU) 2016/680, LED) created a legal framework where the protection of personal data was elevated to an unprecedented level to ultimately avoid any harm, negative impact or unlawful interference made to individuals. Statistics shows this regulatory package has the most direct effect in the rise of confidence in the digital economy. It supported the growth of European digital single market which supported economic growth considera-

11 https://www.coe.int/en/web/data-protection/conference-on-convention-108-as-the-global-privacy-standard-building-a-free-data-transfer-area-while-preserving-human-dignity.

12 Report of the Special Rapporteur on the right to privacy, Report A/73/438, Paragraph 117.e, Page 21.

13 Report of the Special Rapporteur on the right to privacy, A/HRC/40/63, Paragraph 28, page 7.

14 The largest open convention being the Budapest Convention on cybercrime (ETS No. 185) with 68 state parties.

bly.[15]It also furthered economic and political integration of the bloc. At the same time, it shed light to some important questions, including on international transfers and processing of personal data; presented a regulatory approach that emphasizes on security and protective measures against unlawful interference by foreign state's public and intelligence authorities. Another equally important aspect addressed by Convention 108+ is the regulation of Internet big giants. And as already stated in previous sections, the harmonisation of data protection regimes all around the world.

The Committee of Convention 108 believes that Convention 108+ has a good potential to offer viable solutions to the above questions. This is for a very good reason: the EU and its member states always considered the Convention as a bridge between the bloc and the outside world. There are opinions, which this article will not be able to discuss in detail, that this bridge never existed, or even if it existed it was never operational. In fact, the first EU comprehensive framework for data protection, i.e the EU Directive 95/46 in its Recital 11 stated that "*Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention*". The EU current framework for the protection of personal data, i. e. GDPR in its Recital 105 states; "*the Commission should take account of obligations arising from the third country's [...] participation in multilateral or regional systems [...]. In particular, the third country's accession to Convention 108 should be taken into account.*" This sows the synergy between the principles of the Convention 108 and those enshrined in the EU data protection rules, both the old and the current framework.

By inviting any interest on cooperation or on accession from countries beyond Europe, Convention 108 has also attracted interests from African countries. This includes Mauritius, where after signing the Convention 108, it came into force in 01/10/2016. It was succeeded very shortly after by Senegal where Convention 108 entered into force in 01/12/2016, and little later by Tunisia where Convention 108 became applicable since 01/11/2017.

This first wave of accession from African countries was followed by the accession of Cabo Verde where Convention 108 entered force in 01/10/2018 and Morocco where it entered into force in 01/09/2019. Other African countries involved in Convention 108 initiatives include Gabon, Ghana as well as São Tomé and Príncipe who were granted an observer status. Burkina Faso was invited to accede to CoE 108 but has yet to complete the accession process. Furthermore, in addition to the initial

15 https://ec.europa.eu/commission/presscorner/detail/pt/MEMO_15_6385.

engagement in the Convention 108, in 2019, Tunisia signed the modenised Convention, i. e. Convention 108+; and in 2020, Mauritius ratified it.

At the regional level, the Council of Europe has always supported the African Union Convention on Cyber Security and Personal Data Protection (so called Malabo Convention), whose data protection framework and values reflect, in principle, those promoted by the CoE 108 but tailored to fit African countries. In the same vein, the Council of Europe has supported and is continuing to support the Network of African Data Protection Authorities ("NADPA")[16] in their effort to create a truly African network for cooperation, for knowledge and best-practice sharing, for joint actions and for international cooperation, representation[17].

In number of cases (with regard to Nigeria, Kenya, The Gambia, Namibia, Ghana, Gabon, Niger, Sudan, Tunisia, Morocco, Jordan, Uganda)[18] and when countries have expressed their wish to cooperate, the Council of Europe has provided technical assistance through their programmes run by its C-PROC office.[19]Such assistance aimed to support countries to develop national data protection policy, to draft comprehensive data protection laws or to help with the drafting of privacy and data protection strategies. It also carried out activities to empower data protection authorities and to ensure that they can start functioning according to international standards and they can ensure cooperation with its peers in Africa and globally.[20]

D Conclusion

As it transpires from the above, Convention 108+ has tremendous potential, including for African countries. The fact that no other alternatives can be foreseen in the near future at a global level and that like-minded countries need a legal, multilateral instrument for the protection of privacy and personal data if they want to advance their digital agenda, could give enough reassurance for returning benefits for those deciding to invest more resources, energy in it. 31 ratifications by existing state Parties in 5 years of the amending Protocol is a clear and loud signal that this instrument is trusted to deliver upon its entry into force and entrusted to continue

16 https://www.rapdp.org/.

17 https://www.coe.int/en/web/data-protection/monthly-thematic-data-protection-workshops-november-2020-march-2021-online.

18 https://www.coe.int/en/web/data-protection/cooperation.

19 https://www.coe.int/fr/web/cybercrime/cybercrime-office-c-proc-.

20 https://www.coe.int/en/web/data-protection/support-for-the-legislative-process-on-data-protection-in-the-gambia.

to grow in the future. Huge challenges lie ahead as well until it reaches to establish the appropriate level of trust and confidence between all parties but if countries, supervisory authorities and other relevant stakeholders are working together, based on its shared principles and determination, this promise can come true even before one would imagine now.

Part II **African Approaches and Data Colonialism**

Lukman Abdulrauf

African Approach(es) to Data Protection Law

A Introduction

In the last few decades, there has been a significant development in data protection policy and legislative making across the world and in Africa. Africa is now in its third decade of experimentation with data protection law and is noted to have 'the fastest rate of expansion' in data protection laws.[1] This is indeed very significant for the continent considering the slow uptake of technology, which may have led to an equally slower diffusion of data protection laws. So far, more than 36 of the 55 countries in Africa already have data protection laws in place. Some have also moved towards their second-generation data protection law, heavily influenced by European developments with the revision of the GDPR and other data protection instruments. While some see nothing wrong with this, others have questioned whether European-motivated data protection laws suit the African situation. This is so with the resurgence of decolonisation, Af-

Note: Work on this chapter was supported by the U.S. National Institute of Mental Health and the U.S. National Institutes of Health (award number U01MH127690) under the Harnessing Data Science for Health Discovery and Innovation in Africa (DS-I Africa) program. The content of this chapter is solely author's responsibility and does not necessarily represent the official views of the U.S. National Institute of Mental Health or the U.S. National Institutes of Health.

1 Greenleaf/Cottier, *Computer Law & Security Rev.* 2022, 1(2).

https://doi.org/10.1515/9783110797909-005

ricanisation, and 'African solution to African problems' on the continent and their application to various fields of law. As a result of these developments, African data protection scholars are beginning to ask questions such as whether there is now an African approach to data protection law and, if indeed, there is, what it looks like/what its features are.[2] Beyond these, one can ask if there is a need for the movement on specific African approaches, given the level and extent of foreign influence in data protection law and policymaking in Africa. These questions form the crux of this chapter.

There is no gainsaying that data protection laws, unlike many other fields of law, are essentially similar in nature and substance. Almost all data protection laws contain similar principles and core values that guide the use of personal information in the digital age. Most data protection laws define personal information in very similar ways. Irrespective of this, certain countries and jurisdictions have been able to adopt unique approaches in designing and formulating their data protection laws. Sometimes, these approaches are influenced mainly by the philosophical underpinning for data protection law and policy-making or other exogenous and endogenous factors. Scholars have identified United States or European Approaches within this context with idiosyncrasies.[3] While these may not mean a lot, they are used to identify the type of data protection law or policy in a jurisdiction.

This chapter aims to explain whether there is now a unique African approach to data protection law, given recent developments on the continent. If there is no such unique approach, is there a need for one, and what factors should inform such an approach? After the introduction in part A, part B considers the debate regarding approaches to data protection law. What does it mean? How have various scholars approached it? What is its usefulness in practical data protection normative implementation? This part also explains the perspective of the crystallisation of approaches in other jurisdictions like Europe, United States, Canada, and China. Using insights from the discussion in part B, part C focuses on approaches in African data protection law. To determine if a unique African approach has crystallized, it is important to examine trends in data protection law-making in Africa, considering the extent of exogenous and endogenous influence and the uniqueness of data protection laws in Africa. This part concludes that a unique approach is yet to emerge in Africa's current data protection laws. Part D then turns to how Afri-

2 Boshe/Hennemann/von Meding, *Global Privacy Law Rev.* 2022, 56(73).

3 Birnhack, *Computer Law & Security Rev.* 2008, 508; Boyne, *The American J. of Comp. Law.* 2018, 299. See also O'Connor, Reforming the U.S. approach to data protection and privacy, Council on Foreign Relations, 2018.

canisation can be achieved in the context of data protection law in Africa, drawing lessons from various other fields before concluding the chapter in Part E.

It is important to note that in the discussion on approaches, the focus is on the contents of *sui generis* data protection laws and not other instruments or mechanisms for protecting personal information as broadly construed.

B The Perspectives on Approaches in Data Protection Law

In the realm of data protection law, various perspectives emerge regarding approaches. However, these perspectives are rarely critically explained by scholars. This section examines the perspective in which 'approaches' has been used in the scholarship on data protection and argues that there is currently an increasing tendency to use the concept of approaches from a jurisdictional or country-wide context.

I What are Approaches to Data Protection Law

It is surprising that despite the wide use of the concept of 'approaches' in data protection law, what it entails remains unclear. As significant as the concept is, it is yet to be deconstructed in the literature. Literarily, the term approach, among others, means a specific way of considering or doing something[4] or the means or procedure for doing something.[5] In the context of data protection law, therefore, an approach *loosely* entails the means, way, or procedure toward the protection of individuals' personal information. Though broad, this definition implies two things. First, an approach is a means or a specific process, and second, the means and specific process may be different from all other processes. The latter implies some sort of unique style in dealing with an issue. All these conceptions are essential to understand data protection law.

Scholars on data protection law seem to use the concept 'approach' differently. The general understanding, however, is that an 'approach' is the different strategies and framework(s) deployed by governments and organisations to regulate the processing of personal data. Generally, the main approaches widely discussed

4 Cambridge Dictionary Online.

5 Merriam-webster Dictionary Online.

in the literature are comprehensive/government regulatory; self-regulatory/industry or market; co-regulatory/hybrid; sectoral, and privacy by design.[6]

Beyond this general understanding which centres on all the mechanisms and strategies toward data protection, Daniel Solove proposes a more nuanced explanation of approaches that focuses on the design of *sui generis* data protection law.[7] According to Solove, the three general approaches to data protection regulation include privacy self-management, governance, and documentation and use regulation.[8] Solove contends that '[m]ost privacy laws rely predominantly on one of these approaches, with some laws drawing from two or even all of them.'[9] The most common approach is privacy self-management which provides people with the rights to help themselves in controlling the processing of their data.[10] Such rights include the right to notice, access, correction, deletion, etc. This approach generally means that people are responsible for protecting their data by reading privacy policies and notices.[11] The governance and documentation approach is where the law mandates specific governance requirement such as establishing a supervisory authority, conducting data protection impact assessments, documenting incidents, etc.[12] The use regulation approach, according to Solove, is the least commonly employed in data protection law. This approach specifically centres on imposing substantive limitations on utilising personal information, either in general or on a specific type of personal information. It is apposite to state that the GDPR (and its archetypes) is an embodiment of all the three approaches described by Solove. This explains why the GDPR has been considered the world's most influential data protection instrument. Indeed, even Solove unequivocally contends that, although each approach has various strengths and weaknesses, 'to be successful, a [data] privacy law must use all three approaches.'[13]

Solove's explanation of approaches implies a shift in the understanding of approaches in data protection law from the general mechanism towards data protection to a more specific focus on the design of data protection legislation. Indeed,

---

6 See generally Abdulrauf, *The legal protection of data privacy in Nigeria: Lessons from Canada and South Africa*, Unpublished LL.D thesis, 2016, pp 82–90.

7 Solove, *The three general approaches to privacy regulation, 2020.*

8 *Ibid.*

9 *Ibid.*

10 *Ibid.*

11 For criticism of this approach, see Solove, *Harvard Law Rev.* 2013, 1879. See also Solove, *Washington Law Rev.* 2021, 89.

12 For more on this approach, see Waldman, *Washington Uni. Law Rev.* 2020, 97.

13 Solove, *The three general approaches to privacy regulation, 2020.* https://teachprivacy.com/the-three-general-approaches-to-privacy-regulation/#:~:text=As%20proposals%20to%20regulate%20privacy,Use%20Regulation.

the design itself is shaped by various factors and influences. In addition, approaches to data protection law are acquiring a distinct formal character across various jurisdictions, a phenomenon I refer to as the crystallisation of jurisdictional approaches. I will now delve into this matter.

II Jurisdictional Crystallisation of Approaches to Data Protection Law

Data protection law appears to have developed distinct features across different jurisdictions, influenced and shaped by various factors. This has led to the emergence of a discernible jurisdictional identity. While the principles underlying data protection law worldwide are generally similar, there is noticeable diversity in how these principles are integrated into the design and implementation of data protection laws. We can now identify the European,[14] United States,[15] and Canadian[16] approaches and more recently, a Chinese approach.[17]

C Approach(es) to Data Protection Law in Africa

To ascertain the potential crystallisation of an African approach, this section considers the trends observed in Africa's journey with data protection legislation and areas of potential distinctiveness that may be considered as uniquely African.

I Trends in Data Protection Law Making in Africa: The Extent of Indigenous and Exogenous Influences

Although other chapters have considered developments in data protection law in Africa,[18] it is important to preface this discussion with a few reflections on the state of data protection law and policymaking in Africa. A good departure point is the underlying reasons for making data protection laws. Various reasons have

14 Birnhack, *Computer Law & Security Rev.* 2008, 508.

15 Boyne, *The American J. of Comp. Law.* 2018, 299. See also O'Connor, Reforming the U.S. approach to data protection and privacy, Council on Foreign Relations, 2018.

16 Levin/Nicholson *University of Ottawa Law & Tech J.* 2005, 357.

17 Pernot-Leplay, *Penn State J. of Law & Int'l Affairs* 2020, 51.

18 See chapter one – 'Data Governance in Africa: – A Change in Narrative – An Introduction To This Volume', and Chapter four – 'Tech Law as Politics in Africa'.

been proffered for making data protection laws in different African countries. Generally, these reasons include growth in the use of computers to manage state activities,[19] growing activities of private outsourcing entities from European countries,[20] human rights concerns,[21] the need to create a trust for customers, and legal certainty for foreign companies.[22] Other justifications include the concern on surveillance by powerful computer systems.[23] There is therefore no specific overarching concern that has led to the adoption of data protection laws specific to 'all' of Africa. The standard and unifying factor which appears to be the reason for the adoption of data protection laws across the continent is the pressure to satisfy the EU 'adequacy' requirement introduced by Article 25 of the EU Directive for trade purposes. This fact was clearly expressed by the South African Law Reform Commission (SALRC) when coming up with the Protection of Personal Information Act (POPIA) that;

> Privacy is [...] an important trade issue, as information privacy concerns can create a barrier to international trade. Considering the international trends and expectations, information privacy or data legislation will ensure South Africa's future participation in the information market if it is regarded as providing "adequate" information protection by international standards.[24]

Justifications such as the one above has made the influence of European Data Protection Frameworks in Africa both regionally and domestically overwhelming. This influence has been described in critical terms. For example, Boshe *et al.* point to the discourse on 'legal imperialism.'[25] So far, 36 countries have enacted data protection laws. These laws generally adhere to the fundamental framework of data protection legislation, exhibiting minimal deviations or nuances in their implementation. The deviation oftentimes is in the details showing the influence of other data protection instruments, especially that of the EU. Laws generally contain the scope – almost all applicable to both private and public sectors; defines key terms, contain data protection principles (the standard 8 or 9 principles), incorporate exceptions, establish supervisory authorities, and define the scope of their powers and roles, contains provisions on penalties, etc. As mentioned, variation,

19 The reason for the Data Protection Law in Burkina Faso. Greenleaf/Cottier, *Supra*, 14. citing Lo, *La protection des données à caractère personnel en Afrique,* 2017.
20 *Ibid*, Mauritius, Tunisia, Senegal and Morocco.
21 *Ibid.*
22 *Ibid.*
23 See SALRC Discussion Paper https://www.saflii.org/za/other/ZALRC/2009/1.pdf.
24 *Ibid,* p. vii.
25 Boshe/Hennemann/von Meding *supra* 57.

however, exists in the implementation of these laws. While some countries have made notable progress, others are still in the process of finding their footing.

Furthermore, in some countries data protection laws are supported with constitutional provisions which are not homogenous either. It is noteworthy that the countries which have adopted this style have approached constitutional entrenchment differently. While the constitutions in some of these countries contain superficial provisions requiring the government to enact data protection laws,[26] other have very extensive provisions which contain some of the major data protection principles.[27] While the impact of the European influence on this trend cannot be established, this cannot be totally ruled out. The art of constitutional entrenchment of the right to data protection as a right separate from the right to privacy has thick European roots.[28] Elsewhere in Africa, some countries have read data protection right into the constitutional protection of privacy.[29] It appears there is a gradual awareness now, even in some African countries, that data protection protects values that may not be exclusively privacy related. Therefore, in recent data protection laws, the right to privacy is not mentioned as the core of data protection laws.[30]

Many African countries have also established supervisory authorities in line with the requirements of their data protection laws. These bodies are very similar in nature and structure to their European counterparts. However, there are a few remarkable trends in Africa. First, a few countries did not establish independent DPAs in line with international prescripts. Instead, they granted existing regulators the power to regulate and enforce data protection. This is the situation with Eswatini, where the Eswatini Communications Commission is responsible for enforcing the Data Protection Act, 2022; Zimbabwe, where the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) is responsible for enforcing the Data Protection Act; and Rwanda, where the National Cybersecurity Authority

26 See for example, Article 46 of the Constitutional of Algeria, Article 32 of the Constitution of Angola, Articles 1.6 of the Constitution of Gabon.

27 See for example Article 45 and 46 of the Constitution of Cape Verde.

28 See De Hert/Gutwirth, in: Gutwirth/Poullet/de Hert/Terwangne/Nouwt, *Reinventing Data Protection?*, 2009, 3.

29 For example, Section 2 of the POPIA provides that the purpose of the Act is 'to give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations….'. See also Kenya Data Protection Act.

30 For example, the Nigeria Data Protection Bill provides that 'the objective of this Act is to safeguard the fundamental rights and freedoms, and the interests of data subjects, as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999'… See Section 1.

(NCSA) is the supervisory authority of Data Protection Law (Law No. 058/2021).[31] A second noteworthy trend is the time it takes in some countries to establish a supervisory authority after the enactment of data protection laws. For example, Mauritania recently established its Data Protection Authority, that is more than five years after the enactment of its Data Protection Act. On the other hand, countries like South Africa established their Supervisory authority even before the law came into force. In other instances, some countries have established an independent Data Protection Authority in anticipation of formal legislation. This is the case with Nigeria, for example, that established the Nigerian Data Protection Bureau even before a data protection law was enacted.

The regional data protection instruments are also an important source of data protection law in Africa. The ECOWAS Supplementary Act and the SADC Model laws are the most influential regional instruments – the former being the only binding international treaty in Africa. So influential is the ECOWAS Supplementary Act that it is said to have inspired the AU Convention.[32] However, the ECOWAS Supplementary Act (as with the SADC Model Law) has, in turn, been influenced substantially by the EU Directive. A noteworthy trend, which appears to be a welcome development for Africa, is that regional instruments are potentially becoming influential in Africa. Therefore, apart from the inspiration between the ECOWAS Supplementary Act and the African Union Convention of Cyber security and Personal Data Protection (AU Convention), some African countries have also relied on the former instrument in drafting their data protection laws. For example, some provisions of the data protection laws of Guinea, Mali, Niger, and Togo are stated to be 'merely copied and pasted provisions of the [ECOWAS] Supplementary Act.'[33] With the potentially globalising force of the GDPR lately, it is unlikely that African countries trying to enact new data protection laws or amend existing ones will rely on regional instruments. Be that as it may, it is also remarkable that some countries have relied on other African countries to develop their data protection laws.[34]

At the continental level, the AU is becoming more active in data protection. Recently, the AU Convention has just gotten the required 15 ratifications to enable it to come into force, yet, there have been initiatives towards its overhaul.[35] Be that as it may, one of the main criticisms of the AU Convention is the absence of a spe-

31 Recent Developments in African Data Protection Laws – Outlook for 2023, https://www.engage.hoganlovells.com/knowledgeservices/news/recent-developments-in-african-data-protection-laws-outlook-for-2023/.

32 See Greenleaf/Cottier, *Supra,* 1. citing Lo.

33 *Ibid.*

34 Greenleaf/Cottier, *Privacy Law & Business International Report,* 2020, 24–26

35 *Ibid.*

cific body like the European Data Protection Board (EDPB) that is responsible for overseeing its provisions.[36] It should, however, be noted that unlike the EU, the AU is not a supranational institution but rather an intergovernmental body which means there is a limit in which its instrument can be binding on member states.[37] There are, however hopes that the AU Commission may become more active in promoting compliance with data privacy norms and monitor the implementation of its provisions in line with Article 32 now that the Convention is fully in force.[38] The AU also recently adopted a Data Policy Framework, which is a non-binding document that provides guidance for African countries in building a robust data economy.[39] The Framework addresses key issues, including issues of data protection and data localisation.

One noticeable fact in data protection laws in Africa is the dominant external influence. Although there are recent indigenous influences,[40] such influences are insignificant and still shaped mainly by external data protection laws. Hence, it is unsurprising that some African countries have found it more convenient to align themselves with foreign data protection frameworks rather than indigenous ones. For example, out of the nine non-European countries that are parties to the Council of Europe Convention's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 108 (CoE Convention), six are African.[41] Some of these countries have not even ratified the AU Convention.[42] Although this phenomenon has been described as an attempt to "globalize" the CoE Convention,[43] it could make any attempt at an African approach very unlikely. Greenleaf and Cottier argue that 'Drafters of African instruments seems to accept, tacitly or expressly, the necessity to be consistent with other international texts, in particular European instruments.'[44] This is not surprising because aside from economic motivations, European institutions have also provided financial and techni-

36 Boshe/Hennemann/von Meding *supra,* 86.

37 Abdulrauf, *Info. & Comm. Tech. Law.* 2021, 87.

38 See Greenleaf/Cottier, *Supra,* 21.

39 African Union *AU Data Policy Framework* https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf.

40 For example, Republic of Congo Law is heavily inspired by the Data Protection law of Togo.

41 Uruguay, Mauritius, Senegal, Tunisia, Cape Verde, Mexico, Argentina, Morocco and Burkina Faso. See https://www.coe.int/en/web/data-protection/convention108/parties.

42 Morocco, Tunisia, Burkina Faso. See https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf.

43 Greenleaf, *UNSW Law Research Paper,* 2016, 16.

44 See Greenleaf/Cottier, *Supra,* 1.

cal support to countries and international organisations in Africa in making data protection laws.[45]

The Network of African Data Protection Authorities was established to correct some of these anomalies and promote African initiatives. Part of its objectives are 'to promote African legal instruments for the protection of privacy and personal data and ensure their adequacy with the realities of the continent.'[46] As a body with non-binding powers, the extent to which it can be impactful is uncertain.

II Any Unique African Approaches?

From the foregoing, can it be said a unique approach to data protection law has crystallized in Africa? In answering this question, it is essential to engage two perspectives on the issue. The first is if there is an African-wide philosophy, idea, or value that has impacted the formulation and design of data protection laws. The second perspective, which may be influenced by the first, is whether data protection laws in Africa have some consistent style which may indicate the crystallisation of an African approach.

To assess the influence of an African-wide philosophical value on the formulation and design of data protection laws in Africa it is crucial to outline these values briefly. One of the key features of typical African legal systems is legal pluralism implying a fine blend of multiple legal systems.[47] Customary or cultural norms are a very significant aspect in an African legal system and have shaped African responses to various societal issues. Cultural values have also been discussed within the context of data protection values. Without repeating these debates here, it is generally stated that privacy (and hence data protection) in Africa is shaped by a common communalist philosophy informed by cultural values as against individualist values.[48] The extent of the influence of these communalist principles in data protection in Africa is still yet to be established by scholars. For example, after assessing the possible influence of the African philosophy of *ubuntu* vis-à-vis in international privacy models (the EU Directive) on the making of the South African Protection of Personal Information Act, Olinger *et al.* contend that 'both influences would find sufficient expression in the Data Privacy Bill, but that the EU Data Pro-

45 For example, the financial support by the EU to the ITU towards Harmonization of ICT Policies in Sub-Saharan Africa (HIPSSA) project.

46 See Article 5 of the Statutes of the African Network of Personal Data Protection Authorities (RAPDP).

47 See Gebeye, *A Theory of African Constitutionalism*, 2021, 1.

48 For more on this discussions Makulilo, in: Makulilo (ed), *African Data Privacy Laws*, 2016, 3.

tection Directive has the edge in its ability to influence.'[49] The extent of influence of *ubuntu* is based on its strong connection with human dignity, which is one of the core values of data protection law across the world. However, it is arguable that this also has a Western perspective since human dignity has been very significant in shaping the EU data protection framework.[50] Other scholars have also argued that with urbanisation and globalisation, the perceived African values of communism and social cohesion can have little influence on data protection (and even privacy discourses). For example, Makulilo contends that 'urbanism, as well as the influence of modern technologies which came through globalization, has destroyed the social cohesion [in] which individuals were held together in Africa.'[51]

Notwithstanding the above, there are pockets of characteristics with specific data protection laws in Africa, which are arguably a reflection of African traditional values of communalism and approaches to social justice. It must, however, be emphasized that these characteristics are hardly common among data protection laws in Africa. Examples include: The AU Convention's approach of incorporating the rights of local communities.[52] This is probably a derivative of the approach of the African Charter on Human and Peoples Rights (ACHPR) which takes the rights of groups very seriously.[53] The need to protect the rights of groups or 'all people' is probably thought of as a means toward achieving the African-wide philosophy of communalism as against individualism. This may also be a reason for the absence of the right to privacy in the ACHPR.

Another noteworthy aspect that is considered a matter of concern in Africa and has received attention within certain data protection legislation is the safeguarding of vulnerable populations. Indeed, the concerns on vulnerable groups are not limited to Africa alone; however, these matters have recently garnered the attention of human rights advocates and civil society within the African context. These groups are prone to discrimination and bias due to the processing of their data and the outcome of such processing.[54] The GDPR introduced the concept of *vulnerable persons* without clearing what principles need to be deployed to protect their data. Only children, as a significant category of vulnerable groups, have been given elaborate treatments. The influence of the GDPR in this regard is easily noticeable in African data protection laws, which generally focus on children and

49 Olinger/Britz/Oliver, *Int'l. Info. & Lib. Rev.* 2007, 31 (42). 2

50 De Hingh, *German L J.* 2018, 1269–1290. See also Floridi, *Phil. & Tech.* 2016, 307–312.

51 Makulilo, *Beijing L. Rev.* 2016, 192 (203).

52 Articles 8(1) & Article 9(1).

53 See various articles which emphasizes the rights of "all peoples" such as Articles 19, 20, 21, 22 and 24.

54 Malgieri/Niklas, *Comp. L & Sec. Rev.* 2020. See also Malgieri/Fuster *Euro. J. of L. and Tech.* 2022.

leave out other groups such as women, disabled and LGBTQI people. However, some African data protection frameworks have departed from the EU's approach in this respect and provided for some other groups of vulnerable persons. For example, the SADC Model Law recognizes gender as part of sensitive information.[55] It also encourages member states to include other categories of sensitive information that they consider 'presents a major risk to the rights and interests of the data subject, in particular unlawful or arbitrary discrimination.'[56]

Yet another characteristic that may be considered an element of an African approach is the use of alternative dispute resolution (ADR) in resolving data protection issues. Although ADR is not exclusive to Africa, it has often been associated with traditional methods of dispute resolution on the continent before the arrival of Western nations and their legal system.[57] Kenya's approach is remarkable in this respect by introducing ADR to resolve data protection issues.[58] Kenya has also taken this further by making Guidelines for the smooth application of ADR in resolving conflicts between data subjects and data controllers or processors.[59]

A unique approach also is making data protection legislation in African local language. Tanzania's approach is insightful because the Parliament released the official copy of the Personal Data Protection Act 2022 in Swahili.[60] This is a means to promote African values through language and, indeed novel. Although one may argue that Swahili is the national language in Tanzania, English is one of its official languages. Therefore, this initiative could, in a way, be a means to promoting acceptability of the law and national values. The extent to which this may be achieved is however yet to be seen since the law only entered into force recently.

The above is an overview of certain unique features of data protection some data protection framework which are likely to be described as 'African' of 'African-oriented'. However, these are merely isolated features and are rarely common to data protection laws in Africa.

The second perspective in determining the crystallisation of an African approach is to examine whether there is a consistent style or content in data protection laws that might be influenced by a broader African philosophy or value system. This entails exploring if common elements or patterns across these laws

55 Section 19(b) of the SADC Model Law.

56 Section 19(b) of the SADC Model Law.

57 See generally Prince, *Pepperdine Dispute Resolution L. J.* 2018, 393.

58 See section 31 of the Data Protection (General) Regulations, 2021.

59 Office of the Data Protection Commissioner The Alternative Dispute Resolution (ADR) Framework/Guidelines https://www.odpc.go.ke/download/alternative-dispute-resolution-adr-framework-guidelines/?wpdmdl=8328&refresh=647678cbe5d581685485771.

60 http://www.parliament.go.tz/polis/uploads/bills/1664436755-document%20(38).pdf.

reflect shared African principles or values. This inquiry may have been more straightforward if a regional or continental-wide initiative shaped data protection laws in African countries, but as mentioned, this is hardly the case. Many data protection laws in African countries predate regional data protection frameworks and have not established any formal connection with them. The result is the apparent diversity in approaches and style – similar only to the extent that they are a 'transplant' of the EU framework and not an African idea. The effect of 'copying' or 'transplant' in African data protection law has been aptly captured by Boshe *et al.* where they noted that in data protection law, 'there seems to be a tendency to copy or 'transplant' ready-made concepts. A respective approach bears the risk that law is not (any longer, if ever so) the result of (ideally) the mirror of societal conception and values.'[61] Generally, African countries have not shown any homogeneity in their data protection laws beyond the EU influences.

The review of the trend above reveals that a claim to unique African approaches will be difficult to sustain despite the developments on the continent. There is neither a general African philosophical principle or value which has influenced data protection laws, nor have these laws shown any notable trend that can be considered African. After an extensive review of the data protection instruments in Africa, Greenleaf and Cottier concluded that 'The African regional framework does not display any Africa-specific approach to data protection. No traces of less individualist and more communitarian African culture or human rights are found in the texts of these laws.'[62]

Some preliminary explanations can be given for the lack of an African-specific approach. First, African communities, as with their legal systems, do not exist in monolith but rather as a collection of diverse communities. Second, although data protection laws contain very similar principles, different factors have influenced the structure and design of data protection laws in the various African countries. The uniqueness of data protection laws at a general level is not influenced by any common African philosophy or value but rather because most countries have instead found the EU approach to be very influential. Third, the lack of harmonization at the continental level and the low level of influence of the African continental data protection instrument – the AU Convention – will make any attempt to seek a uniquely African approach a practical impossibility.[63] Indeed, several factors make regional harmonization a challenge. Some of the challenges identified

61 Boshe/Hennemann/von Meding *supra,* 68–69.

62 See Greenleaf/Cottier, *Supra,* 1.

63 See generally Amao/Oliver/Magliveras (eds), *The Emergent African Union Law: Conceptualization, Delimitation, and Application*, 2021, where the issue of the general difficulty in achieving harmonization in Africa was elaborately discussed.

by Charles Fombad include a diversity of legal regimes on the continent (civil law, common law, bijural and hybrid systems), heavy reliance on pre-colonial laws in some jurisdictions, conservatism with respect to bridging the gap between the various legal system and language difference.[64] Other challenges are differences in the pace of legal, political, social and economic development, the absence of specialized institutional arrangements in various fields to facilitate harmonisation, and weak, unreliable and inefficient judiciaries.[65]

Besides, the extent of external influence in data protection law would even make a unique African approach even more challenging. All this would therefore lead to a question whether it is even necessary to have a unique African approach to data protection law. Indeed, some will argue that there is no need provided different countries' laws are all geared towards achieving a particular purpose – safeguarding individuals' rights and promoting economic development. Once a data protection law does this, a discourse on approaches is unnecessary. Besides, as mentioned, data protection law, according to many scholars, is said to be centred around certain principles and core values that are similar across the world.[66] Yet another argument against an African approach is the level of contribution of African countries to technological development and the digital economy. Since one of the critical reasons for the development of data protection law is technological advances which have simplified the collection and processing of personal data, the question will always arise regarding the extent of contribution and influence of Africa to the norm creation and agenda setting in data protection globally.

However, other schools of thought, especially those grounded in decolonisation, Africanisation, and promotion of indigenous thinking, will readily oppose such views.

D Africanisation and Data Protection Law: Whither an African Approach?

The discourse surrounding a distinctive approach to data protection proves to be particularly intricate, especially when considering the context of the African continent. This discourse goes beyond simply having data protection laws couched in a similar style or with a unique philosophical basis. It is the proposal of this chapter that rather than thinking of African approaches in establishing uniquely different

64 Fombad, *Africa Today* 2013, 51(56–57).

65 Ibid, 57.

66 See Bygrave, *Data Privacy Law: An International Perspective* 2013, 11.

data protection norms, a better way is to think in terms of the Africanisation of data protection laws.

Africanisation as a concept and a movement has been gaining traction recently on the continent. It is a process of consciously promoting indigenous thinking and knowledge in various facets of life, such as education, politics, economics and culture. Indeed, promoting indigenous thinking could serve many benefits, which include cultural preservation, inclusivity, development and local empowerment. Africanisation movement and ideas are also increasingly gaining momentum in discourses on various legal subjects such as human rights,[67] international law,[68] constitutional law,[69] Intellectual Property Law,[70] and International Investment Law.[71] Hence, African data protection scholars must contemplate the Africanisation of data protection law instead of advocating for an elusive African approach that lacks a well-defined agenda. There are numerous justifications for a renewed call for the Africanisation of data protection law.

To begin with, the realm of African data protection heavily relies on foreign influence and could greatly benefit from a localized viewpoint. Indeed, questions have recently been raised regarding the suitability of the EU GDPR for Africa.[72] According to Cara Mannion, the EU and its 'strict take it or leave it approach' in the GDPR have profound implications for Africa.[73] Through this approach, 'data controllers must either comply with the GDPR's expansive data obligations or risk losing access to the world's largest trading block.'[74] This would instil fear among African nations that perceive the EU as a significant trading partner. According to data from Statista, the EU is Africa's leading trade partner in 2021, with a 23% share of the continent's total trade volume.[75] Furthermore, the total trade value between the two regions was estimated to be about 184 billion Euros in 2019.[76] This makes the costs of failure to comply with the GDPR potentially far-reaching.[77]

---

67 See Viljoen, *International Human Rights Law in Africa*, 2nd ed., 2012.

68 See Gevers, in: von Bernstorff/Dann (eds), *The Battle for International Law: South-North Perspectives on the Decolonization* Era, 2019, 383 (383).

69 Wiebusch, in: Dixon, Ginsburg & Abebe (eds), *Comparative Constitutional Law in Africa*, 2021, 361(361–398).

70 Ncube, *The WIPO J.* 2016, 34 (34).

71 Akinkugbe, *Case Western Reserve J of Int'l L* 2021, 7.

72 Mannion, *Vanderbilt J. of Transnational L.* 2020, 685.

73 *Ibid.*

74 *Ibid,* 693.

75 Africa: main trade partners | Statista https://www.statista.com/statistics/1234977/main-trade-partners-of-africa/.

76 *Ibid.*

77 Mannion, *supra,* 693.

Mannion further contends, 'the GDPR's extra-territorial effects may amount to digital imperialism, allowing the EU to impose its definition of data privacy on African countries without concern for their unique social values and economic realities.'[78] All these have the potential to have a profound effect on the markets of African countries.[79] Taking all these into consideration, it is essential to therefore have data protection laws which reflect local circumstances rather than a wholesome transplantation of foreign principles without critically engaging them and their suitability for individual African countries.

Therefore, Africanisation in data protection law is thinking in terms of 'African solutions to African problems.'[80] Given the seemingly trivial nature of these 'African problems,' it is important that they are taken seriously, especially when considering the prevailing power asymmetries that exist in the data processing operations conducted by foreign entities in Africa. This situation has been described in various manners, such as 'digital colonialism,' 'data colonialism,' or 'algorithmic colonialism,' all highlighting an exploitative dynamic between two entities.[81] This is asides the potential imperialism that is being pushed by the EU using the GDPR – the so-called 'Brussels effects'[82] – and its attendant consequences for Africa. In this light, Africanisation in data protection law is about reframing data protection scholarly discourse and policy agenda to be more Africa-centred.

The next significant question is how Africanisation can be achieved in data protection law. This question, too, adds to the complexity of demystifying the notion of an African approach. However, there are notable preliminary considerations and future research in this area will do well to investigate more deeply into how the various dynamics should play out in practice. First, when Africanising data protection law, it is crucial to delicately strike a balance between international best practices and standards in data protection law while also considering the cultural context and distinct requirements of African society. Since data protection laws are founded on certain fundamental principles, it would not be possible to advocate for a total deviation from those fundamental principles and core val-

78 *Ibid,* 685.

79 *Ibid.*

80 See generally Muchie, in: Muchie/Check/Oloruntoba (eds), *Regenerating Africa: Bringing African Solutions to African Problems* ix.

81 There has been numerous literature discussion some of these kinds of data exploitative relationship with Africa. For example, see Coleman, *Mich. J. of Race and L.*, 2019, 417–439. In the context of health research, see Staunton/Moodley South Afr. Medical J. 2016, 136 and Hennemann (ed) Global Data Strategies, 2023.

82 For more on the Brussels Effect, see Bradford, *The Brussels Effect: How the European Union Rules the World* 2019.

ues. Furthermore, in pursuing Africanisation, it is essential to exercise caution to prevent the isolation of Africa within the global community. Therefore, it is imperative to consider the international context while simultaneously ensuring that local needs are not compromised.

A second consideration in the Africanisation discourse in data protection is regional harmonization. Indeed, regionalism and integration have been clearly identified as one of the most viable means of confronting Africa's greatest challenges.[83] Integration is indeed significant in confronting the threats posed to Africa by foreign big tech entities. Achieving regional integration within the context of data protection law goes beyond the adoption and ratification of the AU Convention and other regional treaties. A focused and intentional endeavour is required to address this issue. With the potential full operationalization of the AU Convention looming, establishing a dedicated body to coordinate data protection frameworks at different levels becomes imperative. The existing disparity between countries and regional initiatives leaves ample room for improvement. A specific data protection body under the AU has the potential to promote further collaboration among member states, which is sorely needy in Africa. The Personal Data Protection Guidelines for Africa 2018 (the Guidelines)[84] recommended the establishment of an 'African-wide data protection committee,' but it appears that the role assigned to the committee is merely advisory.[85]

Thirdly, Africanisation generally involves taking into consideration African cultural values. However, how this may play out in the context of data protection law is still highly contested. For one, the Western versus the African dichotomy in privacy discourse is yet to be defined in Africa and would make it difficult to achieve in practice. The controversy in this regard is only getting started since it is now clear that data protection protects interests that are not exclusively privacy centred. Meanwhile, these discourses are centred around the attitude of the diverse community toward the concept of privacy. Be that as it may, the general idea of how African communities are organised can play a role in some details of the law. The drafters of the AU Convention seem to have considered some of these issues. In its prescription to state parties in establishing data protection framework 'to ensure that any form of data processing respects the fundamental freedoms and rights of natural persons while recognising the prerogatives of State, *the rights of local communities* and the purposes for which businesses were estab-

83 Oloruntoba/Gumede, in: Muchie/Check/Oloruntoba (eds), *Regenerating Africa: Bringing African Solutions to African Problems.*

84 https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf.

85 AU Guidelines, pp 21–22.

lished.'[86] The interests of local communities, too, are considered in defining the scope of the Convention.[87] According to Boshe *et al.* this is a means to reflect the legal culture and cultural diversity within the African continent.[88] Another example from the AU Convention, which arguably reflects African culture, is in the definition of sensitive data where data relating to parental filiation is included.[89] Arguably, this is understood as a ramification of groups' rights and collectivism as opposed to individualism. As much as practicable, more of such values should be included by policymakers in their data protection documents, provided they can make sense of them and how they should be applied.

Fourthly, the Africanisation of data protection law as a means towards an 'African solution to African problem' must prioritize African interests. In this regard, there is a need to promote African businesses and innovation. Intra-African trade should also be taken seriously with the attendant need to develop a robust African digital economy. Robust data protection laws are necessary, but this should not be made to discourage the interaction between countries at the continental or regional level. Therefore, the rules and principles towards cross-border data sharing need must be re-considered in Africa. Drawing inspiration from the EU, it becomes evident how it strategically employs its cross-border data sharing regulations to safeguard and advance European interests. The AU Convention shows insight into Pan-Africanism, thereby providing a good lead where it states, 'The data controller shall not transfer personal data to a non-member State of the African Union unless such a State ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed.'[90] The implication of these provisions is that intra-African data transfers need not satisfy the adequacy requirement. The approach of the AU Convention is similar to what is obtainable in the ECOWAS Supplementary Act.[91] Also insightful is Nigeria's approach, where it identifies 'All African Countries who are signatories to the Malabo Convention 2014' as 'Countries deemed as having adequate data protection laws.'[92] However, some African countries have adopted a contrary approach establishing strict regimes for transborder data flow affecting

86 [Emphasis added]. Article 8(2).
87 Article 9(1)(a).
88 Boshe/Hennemann/von Meding *supra,* 73.
89 Article 10(5)(d).
90 Article 14(6)(a).
91 Article 36.
92 See Annexure C of the Nigeria Data Protection Regulation 2019: Implementation Framework 2020. https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf.

fellow African countries in a bid to satisfy the EU requirements.[93] Some African states, like Botswana, have taken this absurdity further by specifically recognising many foreign countries (primarily European) as automatically having 'adequate' data protection regimes and only two African states.[94]

Fifthly, aggressive public education and enlightenment campaigns are necessary for Africanisation in general. There must be a deliberate effort towards localisation of knowledge on data protection in African communities. The South African Information Regulator is doing a lot in this regard with its aggressive public awareness campaign in local communities using local dialects. Such initiative should be encouraged.

In concluding, Africanising data protection law is, arguably, not about a uniquely different approach to data protection law underpinned by some African philosophical principle or core value. On the contrary, Africanisation is the process of making data protection legislation, policies and practices suitable for the unique cultural, social and economic context of African states. It involves incorporating African perspectives and priorities into the data protection framework to ensure their relevance, effectiveness and sensitivity to the specific needs and challenges of African society. Africanisation is a complex process that requires deep-thinking by the relevant stakeholders. The Africanisation process must begin by acknowledging that a one-size-fits-all approach may not be possible given the diverse realities of African nations. Likewise, the process must acknowledge that breaking away from global best practices is not an option. Therefore, Africanisation should instead focus of striking a balance between global best practices and the specific requirement and aspirations of African countries while promoting inclusivity and contextually fit approaches to data protection. Fortunately, the Africanisation process has started to happen in recent African data protection frameworks. For example, the Personal Data Protection Guidelines for Africa 2018 (the Guidelines)[95] – a joint initiative of the Commission of the African Union and the Internet Society contains Africanisation ideas which are advocated in this chapter. The Guidelines contain a section titled 'The African Context.' The part will be reproduced below for context.

93 See for example, Article 72 of the POPIA, See also Regulation 44 of the Kenya Data Protection (General) Regulation 2021.

94 See Botswana Data Protection Act 2018 Transfer of Personal Data Order 2022 made by the Minister of State President. https://www.dataguidance.com/sites/default/files/botswana_transfer_of_personal_data_order_2022.pdf.

95 https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_2018508_EN.pdf.

> These Guidelines take into account the following characteristics of the African context, as identified by the expert group:
>
> – Significant cultural and legal diversity across the continent, with different privacy expectations.
> – Variations in access to technology and online services, among member states.
> – Sensitivities regarding ethnicity and consentless profiling of citizens, in the context of a nation state.
> – Different levels of capability in areas such as technology and technology-related law and governance.
> – Risks arising from high dependency on non-African manufacturers and service providers:
> – African Union member states' limited ability to influence the behaviour of external service providers.
> – Potentially-increased risk of data misuse where content and services are solely provided by foreign companies (such as "over the top" services or OTTs) and enforcement of local data protection laws may therefore be more difficult.
>
> These factors can increase the difficulty of formulating and enforcing consistent policy among —and sometimes even within—member states.

The above statement presents the most precise and articulate depiction of Africanisation in all African data protection frameworks. In the years to come, it is optimistic that we will witness the manifestation of these ideas in practice. The recent move towards reforming the AU Convention promises to bring some of these ideas into effect.

E Conclusion

The rapid development in data protection law-making in Africa means that the continent can/should now begin to make claims for an identity in the international discourse. This identity will help in many ways to foster ownership, acceptance and respect for data protection norms internally. From the external perspective, African identity in data protection will promote African values, collective voice and influence, human rights and social values, and economic integration and trade. It is also a means to promote Pan-Africanism internationally. However, the processes toward an African identity or approach are controversial. More than three decades of experience with data protection law is not, on its own, enough to justify claims that an African approach has emerged. One must critically interrogate whether data protection laws have been shaped by some unique African values or whether there is some consistent pattern in data protection on the continent. None of these are yet to happen. It is also unlikely that an African approach will crystallize anytime soon. For one, the sheer power of the EU frame-

works and the GDPR and its stronghold on the digital economy will make African countries more inclined to please Europe rather than show some continental identity or affiliation. Besides, issues of an African approach go far beyond mere connection at a policy level between countries to the broader issue of the extent of economic and political integration on the continent. While the African Union can make efforts toward greater regional integration, there is little to which it can do given its current structure. Indeed, unlike the EU, the AU is an intergovernmental and not a supranational institution.[96] The effect is that there is little it can do to ensure African countries comply with its norms.[97] The AU is like a 'toothless bulldog in this regard.[98]

The suggestion is on a need to move beyond the idea of an African approach and consider how to make data protection laws more accommodating of our local circumstances. Ordinarily, there is nothing wrong with legal transplants. The problem is where transplantation fails to take into consideration local circumstances. There is a need for African policymakers to be true to themselves when coming up with data protection laws. Indigenous resources must be leveraged to provide the needed local context. Even where foreign expatriates are engaged, there is a need for locals to partake actively. It is also important that pan-African ideas should always prevail when making these laws. African countries must use their laws and policies to seek solutions to African problems before thinking of impressing the West. Therefore, the proper thinking should be on how to harmonize data protection frameworks at the policy level and then how to Africanize data protection regimes. The recent exploitative dimension in the use of African data further justifies the need for an Africanized, as well as an integrated response. The economic power of foreign big tech companies, which has facilitated data colonialism, means that African countries must unite in response. This can be achieved through the harmonization of data protection frameworks. The first step towards achieving this sort of unit towards counteracting the emerging threats to African countries in the digital economy is to have a formal regional structure equivalent to the European Data Protection Board that will be responsible for coordinating data protection issues on the continent.

With the achievement of the required ratification to come into force, the AU Convention is poised to play a significant role in Africanising data protection. Of course, the Convention is not perfect. However, it can potentially be a useful tool for promoting Pan-Africanism in data protection law and providing a legal

96 Fagbayibo/Owie, *J. of Afi. L.* 2021, 181(200).
97 Abdulrauf, *supra* 87.
98 *Ibid.*

foundation for the regional data protection structure to operate. With time, the Convention can be finetuned towards achieving its intended goal. The current efforts toward revising the Convention cannot go unnoticed, and African leaders must take ownership of this initiative bearing in mind the need to protect and promote African values.

F Bibliography

Abdulrauf, *Info. & Comm. Tech. Law.* 2021, pp. 87–107.
Abdulrauf, *The legal protection of data privacy in Nigeria: Lessons from Canada and South Africa,* Unpublished LL.D thesis, 2016.
Akinkugbe, *Case Western Reserve J of Int'l L* 2021, pp. 7–34.
Amao/Oliver/Magliveras (eds), *The Emergent African Union Law: Conceptualization, Delimitation, and Application*, 2021.
Birnhack, *Computer Law & Security Rev.* 2008, pp.508–520.
Boshe/Hennemann/von Meding, *Global Privacy Law Rev.* 2022, pp. 56–88.
Boyne, *The American J. of Comp. Law.* 2018, pp. 299–343.
Bradford, *The Brussels Effect: How the European Union Rules the World* 2019.
Bygrave, *Data Privacy Law: An International Perspective* 2013.
Coleman, *Mich. J. of Race and L.*, 2019, pp. 417–439
De Hert/Gutwirth, in: Gutwirth/Poullet/de Hert/ Terwangne/ Nouwt, *Reinventing Data Protection?,* 2009, pp. 3–44.
De Hingh, *German L J.* 2018, pp. 1269–1290.
Fagbayibo/Owie, *J. of Afi. L.* 2021, pp. 181–208.
Floridi, *Phil. & Tech.* 2016, pp. 307–312.
Fombad, *Africa Today* 2013, pp. 50–80.
Gebeye, *A Theory of African Constitutionalism,* 2021.
Gevers, in: von Bernstorff/Dann (eds), *The Battle for International Law: South-North Perspectives on the Decolonization* Era, 2019.
Greenleaf, *UNSW Law Research Paper,* 2016.
Greenleaf/Cottier, *Computer Law & Security Rev.* 2022, pp. 105638.
Greenleaf/Cottier, *Privacy Law & Business International Report,* 2020, pp. 24–26.
Levin/Nicholson *University of Ottawa Law & Tech J.* 2005, pp. 357–396.
Lo, *La protection des données à caractère personnel en Afrique,* 2017.
Makulilo, in: Makulilo (ed), *African Data Privacy Laws,* 2016.
Makulilo, *Beijing L. Rev.* 2016, pp. 192–204.
Malgieri/Fuster *Euro. J. of L. and Tech.* 2022.
Malgieri/Niklas, *Comp. L & Sec. Rev.* 2020, pp. 105415.
Mannion, *Vanderbilt J. of Transnational L.* 2020, pp. 685–711.
Muchie, in: Muchie/Check/Oloruntoba (eds), *Regenerating Africa: Bringing African Solutions to African Problems* 2016, pp. ix-xxii.
Ncube, *The WIPO J.* 2016, pp. 34–40.
O'Connor, Reforming the U.S. approach to data protection and privacy, Council on Foreign Relations, 2018.

Olinger/Britz/Oliver, *Int'l. Info. & Lib. Rev.* 2007, pp. 31–43.
Oloruntoba/Gumede, in: Muchie/Check/Oloruntoba (eds), *Regenerating Africa: Bringing African Solutions to African Problems.* 2017, pp. 18–33.
Pernot-Leplay, *Penn State J. of Law & Int'l Affairs* 2020, pp. 49–117.
Prince, *Pepperdine Dispute Resolution L. J.* 2018, pp. 393–418.
Solove, *Harvard Law Rev.* 2013, pp. 1880–1903.
Solove, *The three general approaches to privacy regulation, 2020.*
Staunton/Moodley South Afr. Medical J. 2016, pp. 136–138.
Viljoen, *International Human Rights Law in Africa,* 2nd ed., 2012.
Waldman, *Washington Uni. Law Rev.* 2020, pp. 773–834.
Wiebusch, in: Dixon, Ginsburg & Abebe (eds), *Comparative Constitutional Law in Africa*, 2021.

Mailyn Fidler

African Data Protection Laws: Politics, But as Usual

A Introduction

African countries have taken differing approaches to cybersecurity and data protection regulations, using each category of regulation for a different political purpose. I argued elsewhere that African states have used cybersecurity regulation to resist outside – and primarily European – influence.[1] And the most materially vulnerable African states have been the strongest supporters of an "African solution to African problems" approach towards cybersecurity regulation.[2] But with data protection regulations, something different is happening. African states are not, overall, pursuing African solutions to African problems with respect to data protection. Rather, states with stronger trade ties with Europe—one indicator that a state is materially stronger—are supporting adoption of European approaches.

1 Fidler, in Chesney et al. (eds), *Cyberspace & Instability*; Fidler, Rules as Resistance: Cyber Politics and Africa's Quest for Autonomy (forthcoming manuscript); Fidler, NetPolitics, 2016.

2 This phrase was first coined by George Ayittey, a Ghanaian economist. See Ayittey, Cato Inst. Pol'y Anal., 1994.

https://doi.org/10.1515/9783110797909-006

This difference in approaches between these two contexts can be explained primarily by a key disparity in stakes. With data protection, the European Union (EU) has managed to assert itself as the primary architect of data protection norms. The EU has been able to attach real material consequences to a failure to conform to European regulatory approaches. Gaining or losing European market access is at stake when making choices about data protection laws. With cybersecurity, the material consequences are less direct, allowing African states more room to maneuver. Failing to adopt the Budapest Convention, the European convention on cybercrime, for example, does not come with penalties as clear as losing market access. In other words, the data protection context is one in which African state dependence on outside states is heightened. States with the most to lose —for example, the strongest trade relationships with EU states—will be the most likely to conform. In contrast, the lack of a clear normative leader on cybersecurity allows more room for assertion of African autonomy, so states with the least to lose can afford take bigger risks, including through taking ownership of regulatory structures. Tech laws, even in nondominant states, do politics—just not always the same politics.

B Broad Trends in African Data Protection Law

I Overview of African Efforts

This first section gives an overview of the mechanisms that African states use to regulate technology in general. African technology regulation generally takes place at three levels: the domestic, subregional, and continental level. Subregional efforts refer to efforts by groups of states in regions contained within Africa (West Africa, Southern Africa, etc.). In addition, African states might join in multilateral or international efforts.

Data protection regulation follows this overall structure. At the domestic level, 35 of 55 African countries have officially adopted a data protection law, as of 2023; an additional country, Mozambique, includes data protection provisions only in its constitution, but not in other laws.[3] But between 2010 and 2014, domestic adoption of data protection laws in Africa swung upward and continued to steadily rise from 2014 to 2022.

3 Data Protection Africa, 2023; Hennemann et al. (eds), Univ. of Passau IRDG Research. Paper Series, 2022, No. 22–15; Daigle, J. of Int'l Commerce and Econ., 2021.

At the subregional level, the East African Community (EAC) adopted a model framework for harmonizing cyber law in 2009, which encompassed data protection.[4] The Economic Community of West African States (ECOWAS) adopted a data protection framework in 2010.[5] Unlike its counterparts, this framework is binding on member states.[6] The South African Development Community (SADC) promulgated a model law encompassing data protection in 2013.[7]

Looking at subregional dynamics of domestic adoption, Western African states, followed by Southern African states, generally adopted data protection laws the earliest. North African states are split, with one cluster of states implementing domestic laws quite early, but with a second cluster implementing domestic laws more recently. Central African states fall somewhere in the middle, and East African states have generally implemented domestic data protection laws more recently.

At the continental level, in 2014, the African Union adopted the Malabo Convention on Cybersecurity and Personal Data Protection (Malabo Convention). The Convention entered into force in June 2023 after receiving its 15th ratification.[8] At the international level, African states can be invited to join the 1981 Council of Europe's Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108); the EU's General Data Protection Regulation (GDPR) also has implications for African states. The following subsections address these international and continental regulatory frameworks in more detail.

II The "Brussels Effect" and Data Protection Laws in Africa?

Although privacy is not a strictly European concept, data protection is. European states have been promoting data protection regulation since the 1970s.[9] The European Union continues to be the major agenda-setter for data protection regulation in a way that exemplifies the "Brussels effect." The "Brussels effect" refers to Europe's assertion of "unilateral power to regulate global markets" through "legal institutions and standards."[10] This regulatory power is not purely technocratic; it

4 UNCTAD, 2012.

5 Orji, Comp. Law Rev. Int'l, 2016.

6 ECOWAS 2010, Article II.

7 Harmonization of ICT Policies in Sub-Saharan Africa, 2013.

8 Ayalew, EJIL: Talk!, 2023. This chapter was written before Mauritania's ratification, so the analysis does not include this country.

9 Erdos, European Data Protection Regulation, 2019.

10 Bradford, Northwestern Univ. L. Rev., 2012.

represents a key component of European soft power in the modern age.[11] European states have exercised this power in areas from food safety to environmental regulation.[12]

Data protection is no exception. European actors purposefully and actively seek to export global data protection regulations as a form of power. The two primary European legal institutions that matter to African countries in the data protection context are the Convention 108, refreshed in 2018 (108+), and the GDPR.

The Council of Europe is an international organization distinct from the European Union. Members of the Council do not give up sovereign powers to the Council, but negotiate through the organization to implement common goals. The Council served originally as a precursor to the EU and now sometimes still serves a role as a forum for initial negotiations on topics eventually taken up by the EU.

The Council's Convention 108 was such a precursor. The GDPR is very much modeled on principles embodied initially this Convention. After the 2018 update to the Convention, the two are even more aligned. The Convention is open to requests for accession by non-European states. Eight non-member states have formally joined the Convention. Five of those are African states—Cabo Verde, Mauritius, Morocco, Senegal, and Tunisia—with an invitation extended to Burkina Faso.[13]

The GDPR, despite being formally limited in membership to EU states, also aspires to extraterritorial effect. The GDPR places legal obligations on actors in non-EU countries. The EU adopted the GDPR in 2016 in place of the 1995 Data Protection Directive (DPD). Under the DPD, EU member states had an obligation to ensure that data transferred to non-EU countries was sufficiently protected. Under the GDPR, this burden shifts to the non-EU country. That is, the GDPR contains provisions that apply extraterritorially: non-EU countries processing EU data can be subject to GDPR penalties for failing to protect data according to EU standards.[14] As a result, to maintain (unpenalized) digital trade and interaction with European Union countries, African countries (indeed, all countries) have a strong incentive under the GDPR to at least approximate European data protection standards. The GDPR and the Convention 108+ interact in that acceding to Convention 108+ is one way that non-European countries can signal compliance with the GDPR's approach.

11 See, e.g., Radu et. al., 45 Telecom. Pol'y, 2021.

12 See, e.g., Faulkner, 14 J. of Eur. Pub. Pol'y, 2007.

13 Council of Europe, 2022. Note: Russian Federation is now counted among the non-member signatories since being kicked out, bringing the total to 9. Several additional African states have observer status: Ghana, Gabon, and São Tomé and Principe.

14 Bryant, Stanford Tech. L. Rev., 2021; Hoofnagle et al., Info. & Communications Tech. L., 2019.

C Cybersecurity Regulation as Political Resistance: the "Anti-Brussels" Effect

I The Battle Over Cybersecurity Regulations

We did not see the Brussels Effect fully take hold in the realm of cybercrime and cybersecurity regulation. As with data protection, European states, with the United States, tried to establish a global regulatory gold standard for cybersecurity and cybercrime. In 2001, the Council of Europe, with the United States' and several other countries' participation, launched the Budapest Convention on Cybercrime. The Budapest Convention established a standardized framework for addressing cybercrime, establishing standards intended to harmonize national laws, investigative techniques and cross-border cooperation.

But the goal of being a global gold standard was not realized, at least initially. Global convergence on this document did not quickly or completely happen. Instead, other regional bodies developed their own competing instruments. The Russian-Chinese led Commonwealth of Independent States, to the Chinese-led Shanghai Cooperation Organization, and the League of Arab States each developed their own set of rules for addressing cybercrime, followed by the African Union Convention on Cybersecurity and Personal Data Protection Regulation (Malabo Convention).[15]

The emergence of the Russian and Chinese cybercrime efforts was not particularly surprising in the broader geopolitical context. These forums were pitched as competing alternatives to the Budapest Convention and asserted rival claims to normative leadership in this space. But the African Union Convention (and, to some extent the League of Arab States' effort)[16] cannot be explained in a similar manner. African states are not engaged in an ongoing geopolitical conflict with the West in the same way that China and Russia are. And the Malabo Convention does not differ on key aspects as dramatically as the Russian and Chinese conventions.

In other research, I argue that, instead, the Malabo Convention served as a form of resistance against outside, and especially European, regulation.[17] The Convention was a way for African states, historically more vulnerable than Western states, to assert a degree of autonomy in this new technological issue area. Rule ownership, not just content, mattered. This view of the Convention is supported

15 Benvenisti & Downs, Stanford L. Rev., 2010.

16 For more analysis of the Middle Eastern context, see Shires, 2021.

17 Fidler, in Chesney et al. (eds), Cyberspace & Instability; Fidler, Rules as Resistance: Cyber Politics and Africa's Quest for Autonomy (forthcoming manuscript); Fidler, NetPolitics, 2016.

by the fact that more materially vulnerable states were more likely to support the Malabo Convention, contrary to typical patterns in international relations, turning to legal tools as forms of resistance when more typical avenues of material power are unavailable.

Because this chapter is about data protection laws, I will recap support for this argument only in brief, and only in ways that are relevant to the conversation about data protection laws. The key point to understand is that even though the Malabo Convention addresses cybersecurity and data protection in the same document, the political forces animating support for regulation in these different areas do not entirely overlap. Understanding the political forces that animate African cybersecurity regulation is key to understanding those that animate African data protection regulation.

II The Malabo Convention: "Rules as Resistance"

Theoretical international relations accounts of multilateral mechanisms and signatory patterns all support a view of the cybersecurity portions of the Malabo Convention as tools of resistance against outside influence.

Standard international relations theories fail to account for the creation of the Malabo Convention. Very briefly, the Convention was not a response to material threats—Africa is not a major target of cyber-attacks—nor does it promise to dramatically alter the material power of African states, frustrating a broadly realist account. The Convention is not wildly different substantively from the Budapest Convention, frustrating a constructivist account that would look to normative "African solutions to African problems." The Convention was not a result of interests within countries with the most advanced digital economies lobbying the African Union to adopt a Convention that would best suit their interests, frustrating a liberal intergovernmentalism account. Nor did the African Union itself champion this initiative as a way to elevate its status among similar regional institutions; this Convention was very much driven by member states, frustrating an institutionalist account.

Instead, studying which African countries supported the Malabo Convention revealed that more vulnerable countries tended to support the Convention more. More vulnerable states were using the Convention to resist through rules; staking ownership of rules mattered to these states over and above the benefits that traditional international relations theories look for. These states were pursuing African solutions to African problems through rule ownership.

To identify vulnerable states, I use two proxies. First, I look to colonial history, with French colonial history generally leaving a legacy of greater vulnerability.[18] Second, I look to subsea fibre optic infrastructural development, with fewer cables and fewer landing points corresponding to more vulnerability. A clear pattern emerges on both measures of vulnerability: more vulnerable states tend to support the Malabo Convention. Again, this subverts typical understandings of regionalism in international relations; the most vulnerable states are not typically seen as the drivers of these kinds of efforts.

Overall, these states are not supporting an African convention primarily because of the material benefits it brings, either internationally or domestically. Conversely, these states are supporting the Convention precisely because it contributes to their ability to stake out autonomy, room to maneuver, in a new area. If a state cannot set the terms of its historical and economic relationships with dominant states, and it cannot achieve the infrastructural independence and diversity it would like, it can at least control the rules of the game on its own turf, seeking (if not achieving) governance autonomy.

Tab. 1: Malabo Convention Signatory Status by Colonial History

	French	**British**	**Other**[19]	**Nonstandard**
Signatories	47 %	21 %	32 %	0 %
Non-signatories	31 %	44 %	14 %	11 %
Baseline (Percentage of total countries in Africa with that colonial history[20])	36 %	36 %	20 %	7 %

18 For a lengthier discussion of the merits of using these variables as proxies for vulnerability, see Fidler, in Chesney et al. (eds), *supra* note 13.

19 "Other" indicates a colonial history with any other non-French or non-British colonizer. "Nonstandard" indicates that 1) different areas of the country were under control by different nations at decolonization or 2) the country does not have a history of colonization.

20 Measured as percent of total countries in Africa with a certain colonial history. I am using 55 countries as the total, including the Sahrawi Arab Democratic Republic, where data is available.

Tab. 2: Coastal Malabo Signatories by Undersea Fibre Optic Cable Status

	Cables in 2021	Landing Points in 2021	Cable growth (2017–2021)
Signatories	2,58	1,16	0,58
Non-signatories	3,46	1,53	1,08

In the remainder of this chapter, I focus on trade relations with Europe as an explanatory factor for domestic data protection law (DDPL) adoption. Although trade relations provide a window into DDPL adoption, they shed little light on Malabo Convention signatory patterns (see Tab. 3). Consider only African states that have not signed either Convention 108 or 185. Of those states, Malabo Convention signatories and non-signatories have the same median trade relationships with Europe. So, trade patterns do not give us much insight into the Malabo Convention signatory patterns itself. Some other factor is at work, which, as I have argued above, relates to other measures of vulnerability. But trade relationships play a central role in explaining data protection decisions, as the next Section addresses.

Tab. 3: Malabo Signatory Status by Median Trade Rankings with Europe, of States that have not Signed Conventions 108 or 185

	Median Ranking as Trade Partner of Europe	Median Ranking of Europe as Trade Partner of State
Malabo Signatories	107	2
Malabo Non-signatories	107	2

D African Data Protection Laws: A More Typical International Relations Story

I Introduction to African Data Protection Laws

In contrast, African states *are* using data protection laws to retain or secure material benefits from a theoretical perspective, a realist or liberal intergovernmentalism mostly explains patterns of adoption of African data protection laws.[21] African

21 Moravscik, Int'l Org. 51, 1997; Wendt, Int'l Org. 46, 1992.

states themselves, or interested groups within states, stand to lose materially if African states do not adopt European-style data protection regulations.

Indeed, as I explore below, states for whom that material consequence is likely to be worse—essentially, for whom trade relations are the most important—are more likely to adopt the "Brussels" approach to data protection. States might do so through implementing domestic data protection laws or signing the Convention 108+. The second of these seems to be a stronger signal; states choosing to sign the Convention 108+ generally have even stronger trade relations than states choosing to implement domestic data protection laws.

Given the seeming success of the data protection "Brussels effect", it is tempting to view European actors as the only ones "doing" politics in this arena. They set the agenda, and African states follow. But African states are also "doing" politics here, African states are making political choices to adopt European style laws; indeed, not all countries that could materially benefit from doing so have. The politics of data protection laws just look a little bit more like politics as usual, compared to the resistance politics of African cybersecurity laws.

The following subsections proceed as follows: first, I examine whether domestic data protection law (DDPL) adoption choices can be explained merely as reactions to choices by subregional, regional, or international bodies. The theoretical explanation for that outcome would be a top-down one: countries implement laws domestically in response to outside pressures. I conclude that this story does not fully explain African DDPL adoption. Second, I examine trade relations as a key material variable that can explain, to a substantial degree, African DDPL adoption patterns. Finally, I look at the interplay between vulnerability and resistance—which I argue explains cybersecurity law politics—and trade relations with respect to DDPLs, concluding that trade relations remain the better explanation of DDPL adoption dynamics. The more typical story of states protecting key material interests explains the data protection context.

II Domestic Data Protection Law Adoption Timelines: An Incomplete Explanation

The simplest story supporting a Brussels effect explanation for adoption of African domestic data protection laws would be one where Europe acts, and African domestic adoptions increase in the wake of those actions. Each European initiative, theoretically, could have encouraged African domestic adoption. The GDPR could have encouraged states to adopt domestic laws that would allow them to protect EU data sufficiently to continue to exchange data, and/or sign Convention 108+ to that same end. Alternatively, the African Union's decision to prioritize regula-

tion on this matter could have encouraged signatories to adopt domestic laws in line with the Malabo Convention's requirements. This could provide a different top-down explanation.

But the timeframe when African DDPL adoption ticked up—between 2010 and 2014—is filled with multiple possible triggers (see Fig. 1). African action overlapped with European action in ways that are difficult to untangle. The African Union began drafting the Malabo Convention in 2009 and launched it in 2014. But this African initiative was quickly followed by the launch of the GDPR in 2016 and the revamping of Convention 108 in 2018. It is hard to isolate what portions of that increase came from each initiative based solely on time of adoption. The numbers go up, but it's hard to be certain from what.

Trends are slightly clearer at the sub-regional level (see Fig. 2). For instance, countries in the EAC do not start passing domestic data protection laws until after the adoption of *both* the GDPR and Convention 108+, suggesting that these countries are more sensitive to European regulatory pressure than African pressure. North African countries, too, see more growth after the GDPR's adoption.

But in ECOWAS and to a slightly lesser extent SADC, we see an earlier spike before and after the passage of the Malabo Convention, suggesting these regions were more responsive to internal African debates about data protection regulation. Indeed, the subregional framework in ECOWAS, adopted in 2010, is nominally binding on members, perhaps encouraging adoption. Interestingly, adoption of model laws, whether binding or optional, by subregional organizations seemed to have little immediate effect on domestic adoption. Little growth is seen *immediately* after passage of subregional frameworks, although ECOWAS does see an increase in domestic adoption around 2012/2013.

Taken alone, neither direct responses to European action nor direct repsonses to African institutional actions explain the adoption of domestic data protection laws (DDPLs) in African states. Other variables are at play in explaining the patterns of adoption of DDPLs. The next section examines a key variable—trade relationships with Europe.

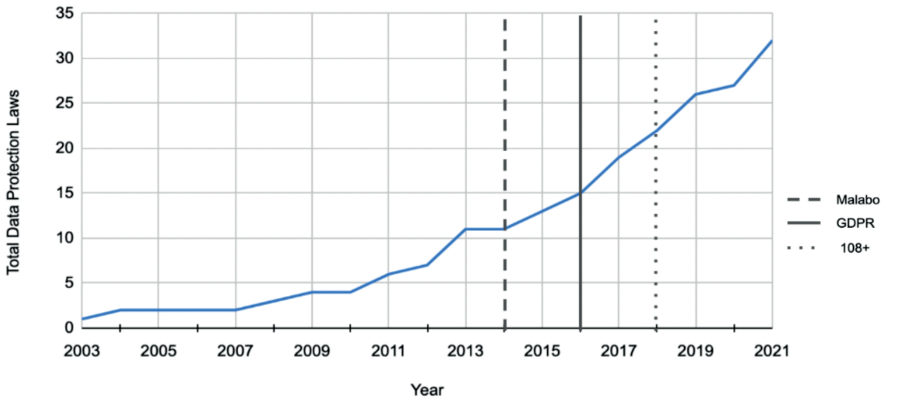

Fig. 1: Growth in African Data Protection Laws.[22]

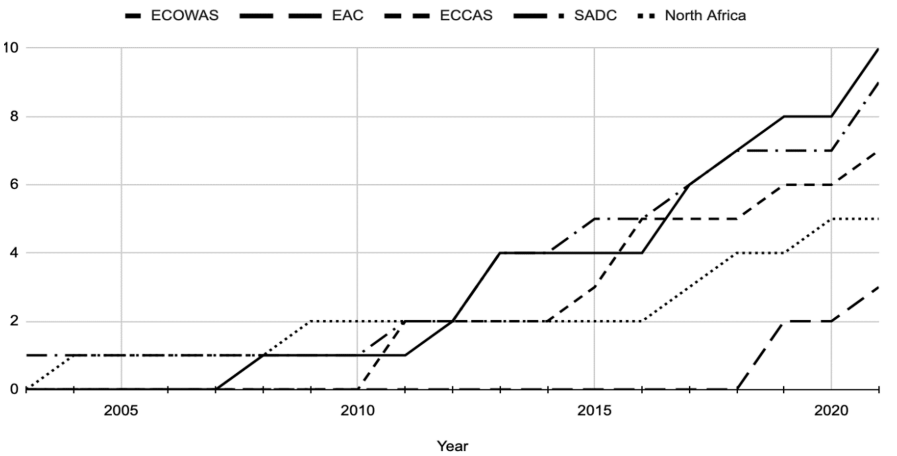

Fig. 2: Regional Growth in Data Protection Laws.

22 I include Mozambique, which only has data protection provisions in its Constitution, in my analysis, given that the political process of renegotiating their constitution to include data protection mirrors some of the same political processes that countries undertake to pass standalone laws.

III Trade Relations: A Better Explanation for Data Protection Choices

Strength of trade relations with Europe demonstrate clear correlations with adoption of DDPLs. A correlation exists between the importance of the trade relationship between the EU and an African country and adoption of data protection legal instruments. Granted, this trade variable is only one of many possible variables. I will pursue other trade-related variables in future work. But for now, consider four categories of African states:

- Category A: African states that have signed the Council of Europe Convention 108+, regardless of the DDPL adoption.
- Category B: African states that have adopted domestic data protection laws, but have not signed any related Convention, whether European or African.
- Category C: African states that have signed the Malabo Convention, but have not signed either Council of Europe Convention, regardless of the DDPL adoption.
- Category D: African states that have taken no legal steps on data protection.

Category A states have the highest median trade rankings with Europe of all of the categories. Category A states are about the 77th most important overall trading partner of the EU (see Fig. 3), and the EU is the most important trading partner of those countries in goods (see Fig. 4).[23] This demonstrates a correlation between states with the most materially at stake through trade and signing the relevant Council of Europe Convention.

Each successive category has lower median trade rankings. Category B states are about 94th most important trading partner of the EU, and the EU is the second most important trading partner of those countries. Category C states are roughly the 107th most important trade partner of the EU, and the EU is also the second most important trading partner of those countries. Last, Category D states are roughly the 131st most important trading partners of Europe, with the EU as the third most important trading partner of those countries.

This pattern supports the theoretical account introduced above. Countries with more materially at stake in terms of trade with European countries seem more disposed to make regulatory choices that conform to European approaches to data protection. The states with the strongest trade relations join the Council of Europe Conventions, and states with the second strongest trade relations pass DDPLs.

---

23 Using median values. Data used comes from Factsheets, Directorate-General for Trade, European Commission, 2022.

The following subsections explore some possible objections and complications to this picture. Particularly, I explore how this explanation interacts with the vulnerability thesis I have advanced regarding signatories of the Malabo Convention. I also address how vulnerability variables do and do not play a role in African data protection decisions.

Future work will explore further ways of examining trade relationships. Trade is complex, and the trade relationships I have used in this chapter are only one of many possibilities.

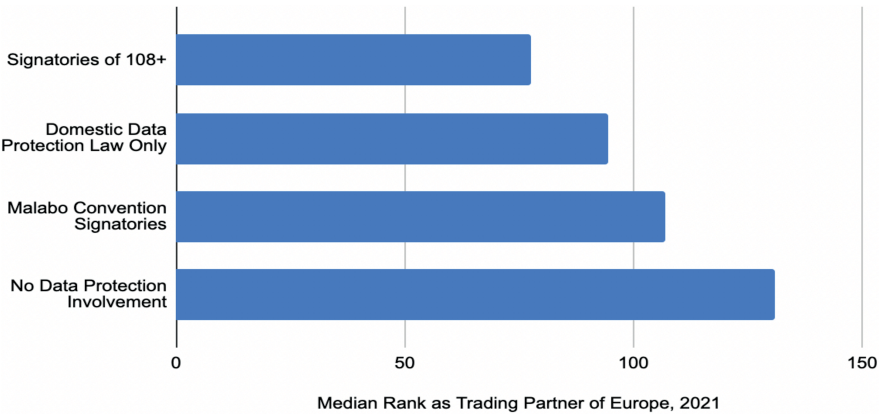

Fig. 3: EU Trade Partner Ranking vs. Data Protection Legal Status.

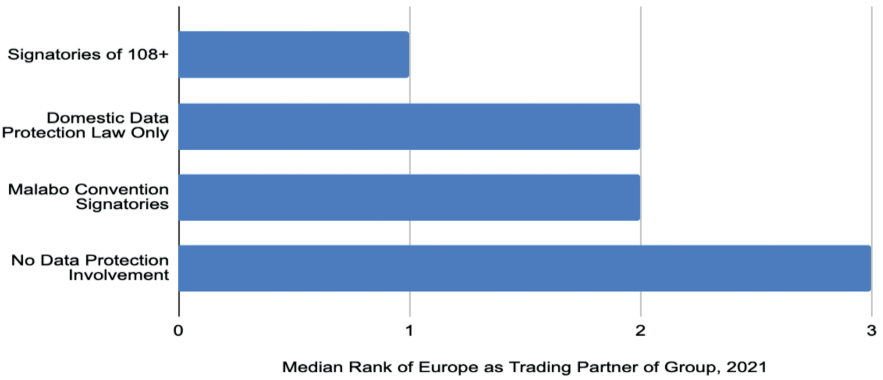

Fig. 4: Rank of Europe as Trade Partner vs. Data Protection Status.

IV Comparing Trade Relations and Malabo Convention Signature as Triggers for Domestic Data Protection Laws

In Section III, Category C represented any state that has signed the Malabo Convention, regardless of whether that state has also implemented a DDPL. This might be obscuring some important dynamics. Let us break Malabo signatories down into two further categories: those that have passed DDPLs and those that have not. Under my explanation, we would expect Malabo signatories that have passed DDPLs to have stronger trade relations with Europe than those that have not passed DDPLs.

Malabo signatories that have implemented DDPLs do exhibit stronger trade relationships with the EU. These states have slightly stronger trade relationships with the EU, compared to states that have signed the Malabo Convention without implementing a DDPL.

This finding is consistent with a view of the Malabo Convention as a tool of resistance on the cybersecurity front and with a view of African data protection regulations as securing material relationships with Europe. The Malabo Convention signatories, as a group, are more vulnerable than non-signatories. But signatories that have implemented DDPLs have stronger trade relationships with the EU compared to signatories that have not. Both dynamics play out.

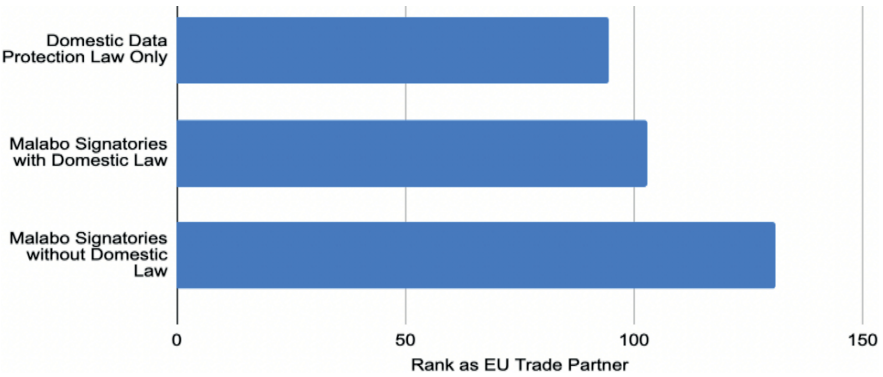

Fig. 5: Domestic Data Protection Laws vs. EU Trade Partner Rank.[24]

24 For each of these groups, the median ranking of Europe as a trade partner of the member states is second.

One might object by arguing that the Malabo Convention had a forcing function on signatories: by signing the Malabo Convention, states are more likely to implement —subsequently—data protection laws. If this were true, African DDPLs could not be seen as a response to European pressure, but rather African pressure.

But the data do not bear this critique out. Most states signing the Malabo Convention already had DDLs in place, suggesting different variables drove decisions to implement DDPLs and sign the Malabo Convention. Indeed, of those states that signed the Malabo Convention, nearly equal numbers of states adopted data protection laws after signing as did not adopt data protection laws after signing, further undermining the theory that Malabo signature drives data protection law adoption.[25]

It is also not the case that merely having a DDPL meant a country is more likely to sign the Malabo Convention: only about 30 percent of the total number of states *with* DDPLs have signed the Malabo Convention.

Tab. 4: Timing of Domestic Data Protection Laws (DDPL) among Malabo Signatories

Legal Status	Percentage
DDPL Predates Malabo Signature	53 %
DDPL Postdates Malabo Signature	20 %
Malabo Signature, no DDPL	27 %

V Comparing Vulnerability Factors and Trade Relations Regarding Data Protection

I have asserted that trade relations play a more important role in explaining African state choices about data protection laws than vulnerability variables do. The data—with one exception—bears this assertion out.

Cable data supports this view. Recall that I used number of undersea cables and undersea cable landing points as one proxy for state vulnerability. Naturally,

25 That said, once a state adopts the Malabo Convention, these dynamics may work differently. For example, the three states who signed the Malabo Convention and then adopted DDPLs have a higher median rank as a European trade partner than the four that signed the Malabo Convention and did not adopt a DDPL yet. But, the median rank of Europe as a trade partner of the countries in the first group is lower than its median rank in the second group.

this data is only available for coastal countries. In the data protection context, coastal countries with more undersea optic infrastructure adopt DDPLs at higher percentages than countries with less. This pattern is the exact opposite of the pattern seen in Malabo signatories, where countries with less cable infrastructure sign the Convention at higher percentages.

My explanation of African state data protection choices—that making pro-data protection choices is a way to protect stronger material ties with European countries—is consistent with this cable finding. Often, Europeans are significant investors in cable infrastructure in African countries with well-developed cable infrastructure. It makes sense that those countries, then, would seek to preserve those relationships through pro-data protection regulatory choices.

Tab. 5: Coastal DDPL Adoption vs. Cable Infrastructure

	Cables in 2021	**Landing Points in 2021**
DDPL	3	1,57
No DDPL	2,15	1,15

Data about historical vulnerability is more complicated. States with French colonial history do make up higher percentages of countries that have passed DDPLs and joined European Conventions than would be expected if colonial history played no special role. This data appears to indicate that more historically vulnerable states, as measured by colonial history, are more likely to pass DDPLs. However, we must also consider that other dynamics might be at play: France itself, for example, may expend more resources in former colonies advocating for data protection laws. For instance, France supported the formation of the Association for Francophone Data Protection Authorities,[26] which has actively supported DDPLs in Francophone countries since its first meeting in 2007. In addition, trade does not completely disappear from this equation. Among states with French colonial history, those that have passed DDPLs have, on average, closer trade relations with the EU (84th) than those that have not passed DDPLs (162nd).

26 Association francophone des autorités de protection des données personnelles.

Tab. 6: Domestic Data Protection Law Passage by Colonial History

	French Colonial History	British Colonial History	Other Colonial History	Nonstandard Colonial History
Countries with DDPLs	48%	33%	18%	0%
Countries without DDPLs	17%	39%	22%	17%
Baseline (Percentage of total countries in Africa with that history[27])	36%	36%	11%	7%

Among African signatories of the Convention 108+, sixty-two percent of signatories have French colonial history, with only twenty-five percent having British colonial history. That's quite a gap; consider that, among African signatories of the Convention 185 (the cybersecurity convention), the numbers are much more similar; fifty percent have French colonial histories and forty percent have British.

With respect to colonial history, then, something different is going on in the data protection realm. Whereas a country with French colonial history might be more likely to support African approaches to cybersecurity law, a country with French colonial history seems to act in the opposite manner in the data protection realm. I hope to dig into this intertwining of colonial history and data protection passage more in future research to better explain this divergence.

Tab. 7: African Signatory Rates of European Conventions by Colonial History

	French Colonial History	British Colonial History	Other Colonial History	Nonstandard Colonial History
Signatories of 108	62%	25%	12%	0%
Signatories of 185	50%	40%	10%	0%

Overall, vulnerability does not tell the full story of African decision-making with respect to data protection law. Examining material relations between states helps explain these patterns better, even though this approach falls short in the cybersecurity context.

27 Measured as percent of total countries in Africa with a certain colonial history. I am using 55 countries as the total, including the Sahrawi Arab Democratic Republic, where data is available.

E Conclusion

The African solution to the African problem of how to regulate data protection appears to be "adopt European approaches". This might feel like an underwhelming conclusion. To the contrary, I want to underscore that this is a political choice that African states are making. Technology laws do political work, in dominant as well as in nondominant states. Here, data protection laws are being used to do the political work of maintaining a material benefit. That is a legitimate political aim, if more pedestrian than using rules as resistance. But the fact that this choice is political should not be overlooked: should the material balance change, African states might make different data protection choices. But at present, the adoption of European-style data protection laws by African states is less a triumph of Brussels right than of Brussels might.

F Bibliography

Ayalew, The African Union's Malabo Convention on Cyber Security and Personal Data Protection Enters into Force Nearly After a Decade. What Does it Mean for Data Privacy in Africa and Beyond? EJIL:Talk! Blog of the European Journal of International Law, 2023.

Ayittey, The Somali Crisis: Time for an African Solution, Cato Institute Policy Analysis, No. 205, 1994.

Benvenisti & Downs, The Empire's New Clothes: Political Economy and the Fragmentation of International Law, Stanford Law Review, 60.2, 2010.

Bradford, The Brussels Effect, Northwestern University Law Review, 107.1, 2012.

Bryant, Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights, Stanford Technology Law Review, 24, 2021.

Chart of Signatures and Ratifications of Treaty 108, Council of Europe, 2022.

Daigle, Data Protection Laws in Africa: A Pan-African Survey and Noted Trends, Journal of International Commerce and Economics, 2021.

Data Protection: Southern African Development Community Model Law, Harmonization of ICT Policies in Sub-Saharan Africa, 2013.

Erdos, The Development of European Data Protection Law and Regulation, in European Data Protection Regulation, Journalism, Traditional Publishers: Balancing on a Tightrope?, 2019.

Factsheets, Directorate-General for Trade, European Commission, 2022.

Faulkner, The political economy of 'normative power' Europe: EU environmental leadership in international biotechnology regulation, J. of Eur. Pub. Pol'y, 14, 2007.

Fidler, Infrastructure, Law, and Cyber Stability: An African Case Study, Cyberspace & Instability (Chesney et al., eds.), 2023.

Fidler, Rules as Resistance: Cyber Politics and Africa's Quest for Autonomy (forthcoming manuscript).

Fidler, Cyber Diplomacy with Africa: Lessons from the African Cybersecurity Convention, NetPolitics, 2016.

Harmonizing Cyberlaws and Regulations: The Experience of the East African Community, UNCTAD, 2012.

Henneman et al. (eds.), Mapping Global Data Law, University of Passau IRDG Resesarch Paper Series No. 22–15, 2022.

Hoofnagle et al., The European Union General Data Protection Regulation: What It Is and What It Means, Information & Communications Technology Law, 28.1, 2019.

Mapping, Data Protection Africa, 2023.

Moravscik, Taking Preferences Seriously: A Liberal Theory of International Politics, Int'l Org., 51, 1997.

Orji, A Comparative Review of the ECOWAS Data Protection Act, Computer Law Review International, 17.4, 2016.

Radu, et. al., Normfare: Norm Entreprenurship in Internet Governance, Telecom. Pol'y, 45, 2021.

Shires, The Politics of Cybersecurity in the Middle East, Hurst, 2021.

Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, Economic Community of West African States (ECOWAS), 2010.

Wendt, Anarchy is What States Make of it: The Social Construction of Power Politics, Int'l Org., 46, 1992.

Part III **Enforcement Aspects**

Iheanyi Nwankwo and Nelson Otieno

Adopting Data Protection Impact Assessment (DPIA) in Africa: Lessons from Kenya's DPIA Framework and Experiences

A Introduction

Several developments have occurred in the African regional data protection regime since 2001 when Cape Verde enacted the first data protection law. Up to 34 African States have enacted data protection laws or regulations, and about 24

https://doi.org/10.1515/9783110797909-007

have set up data protection authorities.[1] Another significant element in these developments is inclusion of the risk-based approach as part of the implementation mechanisms adopted in most national laws. A risk-based approach uses level of risk exposure of data subjects to associate responsibilities with the data controllers and processors.[2] At its highest level, this approach adapts conventional risk management frameworks to data protection. Several commentators have welcomed this approach, especially because it is seen as an avenue of showing accountability by data controllers and processors for their data processing.[3]

Several tools have been advanced for implementing the risk-based approach, one of which is data protection impact assessment (DPIA). A DPIA comprises a process of identifying, assessing and evaluating risks associated with personal data processing, and suggesting measures to mitigate negative impacts on the data subjects.[4] It operates within a defined structure, usually mandated by law. For example, under the General Data Protection Regulation (GDPR), the risk-based approach has been integrated into the basic framework of EU data protection compliance. In this regard, when specific processing involves a high risk to the rights and freedoms of data subjects, a DPIA must be conducted as per Article 35 of the GDPR, following a baseline structure as indicated in Article 35 (3).

Several African States have emulated this approach and included the requirement to conduct a DPIA in their data protection instruments. Kenyan legal framework offers an example of how this tool has been developed into the national system. It has attracted some judicial notice on its importance in data protection and, arguably, one of the recent progressive norms developed by the Kenyan judiciary. Yet, surprisingly, DPIA has not been paid attention to at the African regional and sub-regional levels. Although most of the relevant regional and sub-regional instruments were adopted before the GDPR, arguably, accounting for why DPIA is missing, there seem to be no substantial efforts at reforming them to incorporate the risk-based approach. This raises questions about these instruments' status considering global and regional developments in data protection mechanisms, and how

1 Cf. also Boshe/Hennemann, *Data Protection Laws in Northern Africa – Regulatory Approaches, Key Principles, Selected Instruments*, Konrad-Adenauer-Stiftung e.V., 2022, p. 16.

2 Demetzou, GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved, in: Kosta et al (eds), *Privacy and Identity Management Fairness, Accountability and Transparency in the Age of Big Data,* Springer International Publishing, 2019, p. 137.

3 Centre for Information Policy Leadership, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* 2014; Demetzou, *Comp and sec rev.* 2019, 6 (35); Kuner et al., *IDP law* 2015, 5 (2); Borocz, *EDP law rev,* 2016, p. 467.

4 ICO, Data Protection Impact Assessments 2022.

effectively would they address the risks posed by innovative information technologies such as artificial intelligence.

This paper aims to provide insights into the value that DPIA can offer in the African region. It argues that a carefully crafted introduction and enforcement of a risk-based approach and DPIA tool within the African regional and national instruments would benefit data subjects and provide a fertile ground for data protection authorities (DPAs) to oversee the activities of data controllers and processors within their jurisdictions. Thus, a proactive risk-based approach, including a DPIA mechanism, would enhance data protection at the regional and national levels.

The remainder of this chapter is structured as follows: Section B reflects on the emergence and value of DPIA in privacy and data protection. Section C looks at DPIA's adoption in Africa from regional, sub-regional and national perspectives, while Section D presents data protection in Kenya from inception to its current state, including DPIA implementation. Section E reflects on the previous sections to determine the importance or otherwise of adopting DPIA in Africa. Lastly, Section F gives a conclusion of the chapter.

B The Emergence and Values of Impact Assessment in Privacy and Data Protection

Impact assessment has long been recognised in the privacy sphere, although its historical origin is controversial. Clarke writes that Privacy Impact Assessment (PIA) appeared in 1973 in a Berkeley, California Ordinance.[5] However, other authors could trace its origin to around 1995.[6] Despite this controversy, substantial evidence points in the direction that PIA became mainstream in Australia, Canada, New Zealand and the USA in the 1990s.[7] However, its adoption in the European data protection circle was only traced to the late 2000s.[8] The first indication of

5 Clarke, *Comp. and sec. rev.* 2009, 2 (25), p. 129. A publication from the Canadian Fisheries and Oceans also claims that 'PIAs have been used as far back as the 1970s' without providing any evidence to back this up. See Fisheries and Oceans Canada, *Access to Information and Privacy (ATIP) Procedure Manual*, p. 52.

6 Tancock/Pearson/Charlesworth, *HP Lab.*HPL-2010–63, 2010, 1 (2)10; Flaherty, Privacy Impact Assessments: An Essential Tool for Data Protection. *A presentation to a plenary session on 'New Technologies, Security and Freedom', 22nd Annual Meeting of Privacy and Data Protection Officials, Venice, September 27–30, 2000.*

7 Wright et al, *A Privacy Impact Assessment Framework for Data Protection and Privacy Rights* 2011.

8 Flaherty, *supra.*

using the term PIA in Europe may be implied from the report done for the UK's Information Commissioner's Office (ICO) in 2007. The report suggests that the Data Protection Ombudsman of Finland mentioned PIA in a presentation he made in August of 2007. [9] More apparent evidence of its first application as a regulatory tool in Europe is traceable to the UK's ICO publication of a PIA Handbook in December 2007,[10] where the term 'privacy impact assessment' or 'PIA' was used throughout.

The term 'data protection impact assessment', the literature suggests, first appeared in the Radio Frequency Identification (RFID) Recommendation of the European Commission (EC) in 2009.[11] In this Recommendation, the EC advocated for a 'privacy and data protection impact assessment' to know the implications of RFID applications on protecting personal data and privacy. Since then, the EC appears to have separated the concepts 'privacy' and 'data protection' in impact assessment. EC's subsequent references to the tool from 2010, e.g, in the communication for a comprehensive approach to the revision of the Data Protection Directive,[12] as well as in the Smart Meter Recommendation of 2012, the term 'data protection impact assessment' was used. The term DPIA has crystallised with the adoption of the GDPR and has been used in several EU official documents.[13]

Apart from the above narrative, several supervisory authorities in the EU have made important remarks regarding PIA/DPIA. Notably, before the adoption of the GDPR, in addition to the ICO's PIA Handbook, the French Commission *Nationale de l'Informatique et des Libertés* (CNIL)[14] and the Spanish *Agencia Española de Protección de Datos* (AEPD)[15] also published guidelines on PIA. Since the adoption of the GDPR, several other national supervisory authorities have issued one form of guidance note or opinion on DPIA,[16] including lists of data processing operations that

9 Linden Consulting Inc, Privacy Impact Assessments: International Study of their Applications and Effects, 2007, p. 8.

10 ICO, *PIA Handbook* (version 1.0, December 2007), which was revised in 2009 by *Privacy Impact Assessment Handbook* (Version 2.0, 2009).

11 Recommendation (EU) 2009/387/EG.

12 European Commission, *A Comprehensive Approach on Personal Data Protection in the European Union,* COM (2010) 609 final.

13 See e. g., Directive (EU) 2016/680; Regulation (EU) 2018/1725.

14 CNIL, *Methodology for Privacy Risk Management – How to Implement the Data Protection Act* (June 2012).

15 AEPD, *GUÍA para una Evaluación de Impacto en la de Protección Datos Personales* (2014).

16 Nwankwo, *Towards a Transparent and Systematic Approach to Conducting Risk Assessment Under Article 35 of the GDPR*, PhD Thesis, 2021).

require mandatory conduct of a DPIA according to Article 35 (4) (blacklist) and those that are exempted (whitelist).[17]

Although using PIA to manage privacy risks in the EU was largely voluntary during the defunct Data Protection Directive (DPD) era,[18] it nevertheless attracted attention of several European data controllers. Many organisations adopted PIA as a self-regulatory risk management tool;[19] or as 'one way of proactively addressing privacy principles'.[20] No consensus, however, emerged during this period regarding a systematic procedure for conducting PIA or DPIA. As a result, each data controller devised a suitable method.

Despite this shortcoming, there are many values in conducting a PIA or DPIA, as could be gleaned from the remarks in ISO/IEC Standard 29134:2017:

> A PIA is more than a tool: it is a process that begins at the earliest possible stages of an initiative, when there are still opportunities to influence its outcome and thereby ensure privacy by design. It is a process that continues until, and even after, the project has been deployed.[21]

Several justifications have been advanced for adopting impact assessment in this area. First, conducting an *ex-ante* assessment of the impact of a proposed data processing operation provides an 'early warning system' to assist data controllers and processors in anticipating threats and harms and adopting measures to mitigate them should the anticipated risk occur.[22] This is a proactive approach to compliance. Given uncertainty associated with using communication technologies in personal data processing, DPIA requirement is seen as part of the government's social responsibility to protect the public from potential harm.[23] In this regard, Wright et al. consider PIA an exercise of precaution and a form of risk governance tool.[24]

---

17 EDPB, *Opinions,* https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en (accessed 24 December 2022); see also Nwankwo in: *Turning Point in Data Protection Law*, 2020, 141 (142).

18 The regime of prior checking in Directive 95/46/EC, article 20 and recital 54.

19 Tancock/Pearson/Charlesworth, *HP Lab.*HPL-2010–63, 2010, 1 (2)10.

20 ISO PIA Standard 22307: 2008 for Financial Services (rev 2019).p. v.

21 ISO/IEC Standard 29134:2017, p. vi.

22 Bhargava, *The Shifting Data Protection Paradigm: Proactive vs. Reactive*, https://devops.com/shifting-data-protection-paradigm-proactive-vs-reactive/ (accessed 3 July 2023).

23 Renn *et al.*, *Precautionary Risk Appraisal and Management: An Orientation for Meeting the Precautionary Principle in the European Union*, 2009.

24 Wright et al, Precaution and Privacy Impact Assessment as Modes Towards Risk Governance in: von Schomberg (eds), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, 2011, pp. 83–98.

Furthermore, conducting a proper impact assessment has a competitive advantage. It could render a product or service more attractive to would-be consumers by showing them that potential risks associated with the product or service have been considered and mitigating measures have been baked into the product's architecture. This goes hand in hand with data protection by design because the result of a risk assessment will provide valuable input in the design of a product or service.[25]

Ex-ante impact assessment also allows society to reap the benefits of innovative technologies in a privacy-friendly manner by encouraging developers to engage citizens in decision-making that affects them right from the start.[26] This view is highlighted in the GDPR's provisions requiring data controllers to consult data subjects and the supervisory authorities in appropriate cases during a DPIA.[27]

From a practical perspective, there are actual instances in which conducting a DPIA has been impactful. The Dutch government's assessment of several Microsoft services is an excellent example to buttress this point. The Ministry of Justice and Security of the Dutch government commissioned a DPIA of Microsoft services,[28] the purpose of which was to proactively assess the risk faced by the data subject because of using Microsoft cloud-based services. Such would help put adequate safeguards against the risks of using these services. This initiative found several risks, including that the parties to the contract (the Dutch government and Microsoft) sometimes do not meet the legal requirements. For example, some data that Microsoft initially regarded as non-personal data (e.g. telemetry data, diagnostic data) were indeed personal data because they include, in the case of diagnostic data, 'both behavioural metadata and data relating to filenames, file path and e-mail subject lines'.[29] Microsoft also had a wrong assumption that it was only a data processor in the processing of diagnostic data for some specific purposes. However, the DPIA showed that Microsoft is a joint data controller with government organisations for the particular objectives of the processing.[30] The DPIA also found that 'neither Microsoft nor government organisations have a legal ground' for some purposes for which diagnostic data was processed. Exposing these potential risks before the occurrence of harm shows the value of a DPIA.

25 GDPR Art 25.

26 Som, Hilty and Köhler, *J. of Buss. Eth.* 2009, p. 85.

27 GDPR Arts 35 (9) and 36.

28 These involve Microsoft Office 365 ProPlus, Microsoft Windows 10 version 1.5 and Office 365 online and mobile apps. See Rijksoverheid, *Data Protection Impact Assessments DPIA's Office 365 ProPlus, Windows 10 Enterprise, Office 365 Online and Mobile Apps.*

29 *See* Privacy Company, DPIA Diagnostic Data in Microsoft Office Proplus, 2018, pp. 4–8.

30 *Ibid*, p. 6.

As a result, Microsoft had to amend its service, putting the relevant safety measure in its offerings to the Dutch government.

Furthermore, the DPIA conducted by the same institution against the use of Google G Suit Enterprise found ten high data protection risks and suggested mitigating measures against those risks.[31] One threat was that Google and government organisations using their services had access to audit log files containing diagnostic data about end-user behaviour. These log files could potentially be used to create a profile of the G Suite end-users. The DPIA noted a risk that if the diagnostic data is accessed unlawfully, there could be blackmailing and stalking of employees or other data subjects based on such data. Furthermore, it was also identified that Google frequently uses settings that maximise data processing by default instead of minimising it. Eventually, Google had to implement risk-mitigating measures suggested in the DPIA and resumed supporting government services.[32]

At the height of the COVID-19 pandemic, there were calls for digital solutions to enhance contact tracing in Europe. As a result, the Corona App was developed as a technical solution. The App had a contact tracing feature that could process personal health data on a large scale. When the developers of the App failed to publish a detailed DPIA, a group of scientists and data protection experts conducted a DPIA in line with the requirement of Article 35 of the GDPR as a proactive contribution to the debate.[33] This DPIA revealed numerous weaknesses and risks in the App framework, including defective legal basis, insufficient purpose-binding and improper anonymisation. Several technical and organisational measures were suggested to improve the app design.

Today, sector-specific DPIA rules are emerging to ensure protection of personal data in several circumstances, such as DPIA for smart grid and smart metering environments,[34] and the RFID PIA framework.[35] In addition, software versions of DPIA tools have also emerged, such as the CNIL's PIA software,[36] and the AEPD

31 Rijk, *DPIA Google G Suite Enterprise,* 202, p. 149.

32 *See also* Speed, *Dutch Public Sector Gets Green Light to Use Google Workspace*,30th May 2022, https://www.theregister.com/2022/05/30/google_workspace_dutch_government/ (accessed 10 January 2023).

33 Bock et al., *Data Protection Impact Assessment for the Corona App*, 2020.

34 European Commission, *Data Protection Impact Assessment for Smart Grid and Smart Metering Environment,* https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en (accessed 12 January 2023).

35 *BSI, Technical Guidelines, RFID as Templates for the PIA-Framework,* 2010.

36 CNIL, *The Open Source PIA Software Helps to Carry Out Data Protection Impact Assessment*, 2021.

web-based DPIA evaluation tool.[37] Furthermore, automation is gradually gaining ground in this area, and the ISO has published a standard for conducting a PIA.[38] Undoubtedly, as the examples above show, proactively deploying the DPIA tool has several positive impacts in the protection of personal data. The next section examines DPIA adopted in Africa, looking at the regional, sub-regional and national environments.

C DPIA Adoption in Africa

I Regional and Sub-regional Frameworks

There have been several remarkable developments in the area of privacy and data protection at both the regional and subregional levels in Africa. The African Charter on Human and People's Rights does not contain a provision on the right to privacy or data protection. At the regional level, e.g, some key instruments, such as the Convention on Cyber Security and Personal Data Protection (Malabo Convention),[39] and the Declaration of Principles on Freedom of Expression and Access to Information in Africa,[40] address data protection in different scopes. There are other non-binding documents that contain privacy provisions, such as the African Declaration on Internet Rights and Freedoms,[41] and the African Union (AU) Digital Transformation Strategy for Africa (2020–2030).[42]

37 AEPD, *GDPR Risk Assessment,* https://evalua-riesgo.aepd.es/index_en.html (accessed 15 November 2022).

38 ISO/IEC Standard 29134:2017.

39 African Union *Convention* on *Cyber Security* and *Personal Data Protection 2014* (Malabo Convention).

40 Declaration of Principles on Freedom of Expression and Access to Information in Africa (Adopted by the African Commission on Human and Peoples' Rights at its 65th Ordinary Session held from 21 October to 10 November 2019 in Banjul, the Gambia).

41 African Declaration on Internet Rights and Freedoms 2014.

42 AU Digital Transformation Strategy for Africa 2020–2030.

However, a critical analysis of these instruments indicates that the risk-based approach and DPIA have not been utilised. They neither consider this approach nor contain any requirement for DPIA. While the Malabo Convention includes a security requirement, it rather contemplates adopting "appropriate precaution" in dealing with data security.[43] Notably, the Personal Data Protection Guidelines for Africa 2018 issued by the Internet Society and the Commission of the AU recommends that organisations adopt risk-based approaches in evaluating the likelihood and impact of risks on personal data.[44] However, this document is a mere guidance document without any binding effect. Similarly, the IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa 2021 recognises DPIA as a compliance tool.[45] This non-binding and practitioners'-specific guide emphasises on the value of DPIA as a risk management measure and shows how it could be structured.

Lack of utilisation of risk-based approach is also seen within the African sub-regional frameworks. For example, only the Southern African Development Community (SADC) Model Act on Data Protection[46] contains a provision requiring data controllers and processors to consider the potential risk of processing operations to the data subject as part of data security obligations.[47] However, the Model Act does not contain any explicit provision on DPIA. Other key African sub-regional instruments on data protection, such as the Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection;[48] and the East African Community (EAC) Framework for Cyberlaws,[49] have no provisions for a risk-based approach or DPIA. Despite this lacuna, emerging national frameworks seem promising; several national instruments have adopted the risk-based approach and DPIA tool in various guises, as will be shown in the next sections.

43 Malabo Convention Article 21.

44 Personal Data Protection Guidelines for Africa 2018, p. 14.

45 International Bar Association, *The IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa*, 2021, p. 42.

46 Southern African Development Community (SADC) Model Act on Data Protection (2013).

47 *Ibid,* Article 24 (2). Other provisions mentioning risk in the relevant context in the SADC Model Law include Articles 26 (3), 27(1) and (3), 28(1), 31(3).

48 Supplementary Act A/SA.1/01/10 (http://sa.1/01/10) on Personal Data Protection with ECOWAS, 2010.

49 EAC Framework for Cyberlaws, 2008.

II National Frameworks

As earlier indicated, several data protection laws and bills exist in African States. A few countries have even amended their initial laws to reflect technological and regulatory development globally.[50] A remarkable feature of these laws is that they have been influenced to a large extent by international and other regional developments, particularly Europe. Greenleaf and Cottier have underscored this influence, pointing out that European instruments such as the GDPR, Convention 108 and the defunct DPD have reflected heavily on the African national data protection frameworks.[51] As such, several principles, obligations and rights found in the European framework have been transplanted into the African setting in various guises, including the risk-based approach and DPIA.

An analysis of these African national laws shows a significant presence of the risk-based approach and DPIA. However, there are differences concerning their characteristics, including how this obligation is introduced into the legal system. In some cases, several similarities exist, which can be explained by the fact that several African instruments were adapted from the GDPR. In most cases, the principal data protection law explicitly introduces the obligation to conduct a DPIA. Kenya, Mauritius, Malawi, Rwanda, Zambia, Cape Verde, the Republic of Congo and Benin are examples of those countries. In some other cases, the obligation to conduct a DPIA is implied from some provisions in the principal legislation, especially the data security provisions requiring data controllers and processors to adequately safeguard personal data by considering the risk posed by a processing operation. This approach is seen in Ghana, Lesotho, Nigeria, South Africa, Uganda, Zimbabwe, Benin, Eswatini, Botswana and Algeria. Remarkably, in South Africa, Nigeria, Angola, Madagascar and Uganda, the requirement to conduct a DPIA was later introduced explicitly through implementing guidelines or other regulations issued by regulatory authorities. Finally, it is worthy of mention that in Morocco, where there is neither an explicit nor implied provision requiring data controllers to conduct a DPIA, the supervisory authority has introduced it through Deliberation No. D-188–2020 of 14 December 2020. In Ivory Coast, there is no provision requiring the conduct of a DPIA in the main law, but DPIA is mandated by the supervisory authority as a good practice for processing sensitive data.[52]

---

50 For example, Cape Verde, Mauritius and Mali. *See* Boshe/Hennemann *supra.*

51 Greenleaf/Cottier, *Comp. and sec. rev.*, 2022, p. 44.

52 Ollivier, Ivory Coast – Data Protection Overview, 2022, https://www.dataguidance.com/notes/ivory-coast-data-protection-overview (accessed 17 November 2022).

Other African countries that could be said to have inherited the requirement to conduct a DPIA are parties to the Council of Europe Convention 108+.[53] This Convention introduces DPIA under Article 10.[54]

Tab. 1: Sample of DPIA Provisions in African National Data Protection Laws[55]

	Country	Data Protection Instrument	Provision on DPIA	Remarks
1	Kenya	Data Protection Act 2019	Section 31 (1)	Explicit requirement
2	Mauritius	Data Protection Act 2017	Section 34	Explicit requirement. Mauritius has also signed and ratified the CoE Convention 108+
3	Ghana	Data Protection Act 2012	Section 28	Implied requirement
4	Lesotho	Data Protection Act 2011	Section 20	Implied requirement
5	Malawi	Data Protection Act 2022	Section 24	Explicit requirement
6	Nigeria	Nigeria Data Protection Regulations 2019 (NDPR); NDPR Implementation Framework 2020	Article 4.1(5) (NDPR) Para 3.2(viii), 4.2	NITDA indicates that conducting a DPIA could be implied from Art 4.1(5) NDPR. However, the obligation is introduced as an explicit requirement in the NDR Implementation Framework.
7	Rwanda	Law relating to the protection of personal data and privacy, N° 058/2021 of 13/10/2021	Article 38	Explicit requirement
8	South Africa	Protection of Personal Information Act 2013; Regulations Relating to the Protection of Personal Information (2018)	Section 19 (Act); Section 4 (Regulation)	DPIA is an implied requirement under the POIA but introduced explicitly in the Regulations

53 Convention 108 + Convention for The Protection of Individuals with Regard to The Processing of Personal Data.

54 Although Cape Verde, Mauritius, Morocco, Senegal, and Tunisia, ratified Convention 108, only Mauritius and Tunisia have signed Convention 108+. Mauritius has gone further to ratify it. *See* Chart of signatures and ratifications of Treaty 108.

55 Note that this table does not include all African States. While no clear evidence of express or implied DPIA obligation is seen in some principal data protection laws such as in Egypt, in other cases, the authors could not confirm the current state of the laws due to difficulties in accessing the relevant instruments.

Tab. 1: Sample of DPIA Provisions in African National Data Protection Laws *(Continued)*

	Country	Data Protection Instrument	Provision on DPIA	Remarks
9	Uganda	Data Protection Act 2019 Data Protection and Privacy Regulations, 2021	Section 20(2) (Act); Section 12 (Regulations)	DPIA is an implied requirement under the DPA but introduced explicitly in the Regulations
10	Zambia	Data Protection Act No. 2 of 2021	Section 46	Explicit requirement
12	Zimbabwe	Data Protection Act No. 5 of 2021	Section 20, 21	Implied requirement
13	Morocco	Law No. 09–08 Deliberation No. D-188–2020 of 14 December 2020	No Provision Page 3 of the DPIA Deliberation	The primary data protection law does not contain any provision regarding DPIA. However, Deliberation No. D-188–2020 of 14 December 2020 incorporates DPIA.
14	Benin	Law No. 2009–09 of May 22, 2009, Dealing with the Protection of Personally Identifiable Information (Law No. 2009–09)	Section 50	Implied requirement
15	Ivory Coast	Law 2013–450 of June 19, 2013, Relating to the Protection of Personal Data	No provision	However, ARCTI is beginning to impose it as a good practice for processing sensitive data
16	Cape Verde	Law No. 121 /IX/2021 (amendment to the Law No. 133-V-2001)	Article 16-D	Express requirement
17	Republic of Congo	Law 29–2019 on the Protection of Personal Data	Article 79	Explicit requirement
18	Algeria	Law No. 18–07 dated 10 June 2018 Relating to the Protection of Individuals in the Processing of Personal Data	Article 38	Implied requirement
19	Tunisia	Obligation as a party to Convention 108+	Article 10 (2)	Explicit requirement under Convention 108+ which Tunisia has signed
20	Eswatini	Data Protection Act 2022	Article 14 (2)	Implied requirement
21	Botswana	Data Protection Act 2018	Article 32 (2)	Implied requirement
22	Angola	Law 22/11 on the Protection of Personal Data	Article 30 (2)	Implied requirement

Tab. 1: Sample of DPIA Provisions in African National Data Protection Laws *(Continued)*

	Country	Data Protection Instrument	Provision on DPIA	Remarks
23	Madagascar	LOI N° 2014–038 *Sur la protection des données à caractère personnel*	Article 15	Implied requirement. Note that under Article 46, the supervisory authority shall authorise processing operations that present specific risks
24	Benin	Loi n° 2017–20 *portant code du numérique en République du Bénin.*	Article 428	Express requirement

It is important to point out that some of the data protection bills under legislative consideration in several African States, including Nigeria[56] and Namibia,[57] contain explicit DPIA provisions. This is a positive development. It is suggested that other nations emulate this when either amending their existing laws or enacting new ones. The next section takes a deep dive into Kenyan approach in implementing the DPIA framework.

D DPIA in the Kenyan Data Protection Framework

I Kenya's Legal Path to Data Protection Law

1 Independence Constitution and its Implications to Privacy Right Development

On 12 December 1963, Kenya attained independence after Her Majesty the Queen of United Kingdom issued the Kenya Independence Order in Council of the same year. Schedule II to the Order in Council contained the (Independence) Constitution of Kenya. The Second Chapter of the Constitution provided for the protection of fundamental rights and the freedoms of the individual. Notably, the right to privacy was not expressed in this Constitution.

56 Nigeria Data Protection Bill 2022, clause 29.

57 Namibia Draft Data Protection Bill 2022, clause 5(1)(j).

With independence, Kenya joined the United Nations (UN). The UN membership meant that Kenya subscribed to the Universal Declaration of Human Rights (UDHR), which guaranteed the right to privacy. The express privacy protection under this non-binding instrument filled the gap in the Constitution. The protection was firmed up in a legally binding instrument in 1966 when the UN adopted the International Covenant on Civil and Political Rights 1966 (ICCPR).

In 1973, the US Supreme Court gave a landmark ruling that 'due process guarantees' protected the right to privacy.[58] This ruling had a huge persuasive effect in Kenya.[59] Its application to Kenya meant that Article 20 of the Independence Constitution, which guaranteed protection against arbitrary searches, could also be extrapolated to include a guarantee for the right to privacy.

However, in the 1980's, when the UN Human Rights Committee advocated for the protection of personal data as part of the right to privacy,[60] Kenya encountered challenges. The challenges included a lack of awareness of privacy rights and a lack of clarity on the domestic effect of the international conventions. There was also no robust constitutional protection of the right to privacy.[61]

In 2010, Kenya voted for and promulgated a new Constitution which repealed the Independence Constitution. Article 31 of the new Constitution protects the right to privacy, which includes the protection of personal data.[62] The Constitution further provides for court actions as means of implementing the right to privacy.[63] It also required Parliament to legislate on an enforcement framework for the right to privacy. In addition, the Constitution also recognised that international conventions like ICCPR, to which Kenya is a part, would apply directly to Kenya's domestic legal system.

2 Statutory and Judicial Developments between 2010 and 2019

Kenya's statutory landscape has also developed in response to the changing environment and scores of concerns on the misuse of personal data. As early as the late 20th century, the Kenya Information and Communications Act 1998 was enacted to

58 *Roe v Wade* 410 U.S 113.

59 *PAK & another v Attorney General & 3 others* (Constitutional Petition E009 of 2020) [2022] KEHC 262 (KLR) (24 March 2022) (Judgment), para 73.

60 By 1988, the UN Human Rights Committee had recognized the need for data protection laws to safeguard the fundamental right to privacy.

61 Judicature Act 1967.

62 Kenyan Constitution 2010, Art 31(a)-(d).

63 *Ibid,* Arts 22 and 23.

regulate telecommunication services, broadcasting and postal courier services and related issues. In 2009, an amendment to this law, introduced a further protection against surveillance and communication interception. The Kenya Information and Communications (Consumer Protection) Regulations 2010 also required telecommunication operators to put in place both technical and organisational measures to safeguard the security of their services,[64] and prohibit monitoring or disclosing the contents of subscribers' communication.[65]

In 2012, Parliament introduced the Data Protection Bill 2012.[66] The Bill required DPIA to be conducted in case of high-risk processing.[67] The Privacy and Data Protection Policy 2018[68] also addresses the obligations of data controllers to conduct DPIA.[69] Ultimately, the Data Protection Bill was revised in 2019 after consideration by Parliament.[70] It was then enacted into law in November 2019. Section 31 of the Act requires data controllers and processors to conduct DPIA when they engage in high-risk processing of personal data.

Besides law-making, there has also been several court cases on alleged breaches of various aspects of Article 31 of the Constitution of Kenya of 2010.[71] This has resulted in a gradual development in this area of law in the period leading to and after 2019 when the Data Protection Act was passed.

64 Kenya Information and Communications (Consumer Protection) Regulations 2010, reg 4(1).

65 *Ibid*, reg 15(1).

66 Data Protection Bill 2012, clause 21(2)(d).

67 *Ibid*, clause 27(3).

68 The Policy expressed the Government's strategy of addressing the privacy concerns of the citizens taking a cue from international human rights law and the constitutional guarantees in Kenya at the time (*See* Privacy and Data Protection Policy 2018, p 4).

69 Privacy and Data Protection Policy 2018, para 8.2.9.

70 The Departmental Communication, Information and Innovation, Report on the Consideration of the Data Protection Bill, 2019 (October 2019), paras 93–94.

71 *See Bernard Murage v Fineserve Africa Limited & 3 others* [2015] eKLR; *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others* [2018] eKLR; *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Society & 8 others(Interested Parties); Centre for Intellectual Property & Information Technology (Proposed Amicus Curiae)* [2019] eKLR (*Nubian Rights Forum & 2 others v Attorney-General*); *Ex-parte Katiba Institute & Another Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested Party)* (Judicial Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review) (14 October 2021) (Judgment).

3 Kenya's DPIA Regulatory Framework

The Data Protection Act of 2019 (the Act) provides key principles and obligations for data protection as well as rights of the data subjects. It also prescribes the rules for various scenarios of data processing. Furthermore, it prescribes certain self-regulatory mechanisms for data controllers and data subjects. Lastly, it provides institutional frameworks for its implementation.

Under section 31(1) of the Act, DPIA is not mandatory. It is only conducted in instances where a processing operation is likely to result in a high risk to the rights and freedoms of the data subjects. This requires data controllers and data processors to conduct threshold assessments to determine existence of high risks in their (proposed) data processing having regard to the nature, scope, context, and purposes of the data to be processed.[72]

DPIA is conducted to assess the impact of envisaged processing operations on protecting personal data. Section 31(2) to (5) of the Data Protection Act provides for minimum requirements and procedures to conduct a DPIA. They include a description of data processing operations and purpose of the processing; assessment of necessity and proportionality; assessment of the risks and development of risk mitigation measures risks, safeguards and other mechanisms for protecting personal data in compliance with the Act. Additionally, the Act requires that ODPC to be consulted if a DPIA shows residual risk.

The Cabinet Secretary for the ICT and Youth Affairs has developed three regulations to give effect to the provisions of the Act. Data Protection (General) Regulations 2021 is more relevant to DPIAs. The Regulations complement section 31 of the Data Protection Act in many ways. For example, part VII of Regulation 2021 lists the processing activities that require DPIA (blacklist). Also, part V of the Regulations expounds on privacy by design and by default, prior consultation with the ODPC, and DPIA reporting and audit processes which are key steps in conducting DPIA process. The Third Schedule to the Regulations provides a template for conducting a DPIA.

In sum, Kenya's DPIA framework resembles the procedures under the GDPR. This is seen in the language, structure, and content in both frameworks. For example, both indicate that a DPIA must be conducted mandatorily (only) in cases where there is a high risk of processing personal data. Both also contain minimum

72 Data Protection Act 2019, s 31(1). Under s 51(1)(a)-(c), there are exempted operations for which a threshold assessment is not necessary. They are processing operations by individuals in the course of purely personal or household activity, processing for national security and processing action in respect of disclosures that are required by written law or by an order of the court.

requirements of the DPIA process and accommodate blacklist and whitelist of operations requiring or not requiring DPIA. However, there are also some notable differences between the two frameworks: under the Kenyan DPIA framework, unlike the GDPR, there is no prescription for seeking views of data subjects or other stakeholders in the DPIA process.[73] Also, the obligation to conduct a DPIA is put on to both data controllers and data processors.

II Implementation of DPIA in Kenya: Prospects and Challenges

1 Organisation of the ODPC

Successful implementation of the DPIA framework highly depends on the supervisory authority's capacity, independence, and competence. From the lens of institutional capacity, the ODPC is central to several activities around DPIA, such as consultation on residual high risks processing, receiving DPIA reports, and making binding recommendations on the report. In addition, the ODPC has a discretionary role of publishing DPIA reports on its website.[74]

Although the ODPC is newly established and facing some initial hurdles, it has taken steps to organise itself and establish physical offices. The Data Commissioner has been appointed since October 2020.[75] Since then, the ODPC has developed an institutional structure with Directorates. Directorates' activities and goals are aligned with the Strategic Plan 2022/2023 to 2024/25.[76] The ODPC has also taken steps to sort out the capacity issues in the Directorates by recruiting staff in those Directorates.

Overall, the ODPC aims to enhance public trust and transparency as well as foster stakeholder confidence through the various activities it has initiated since its inception.[77] It launched its new website and logo in February 2021.[78] The user-friendly website also links key instruments, including those that guide con-

73 GDPR Article 35(9).

74 Data Protection (General) Regulations 2021, reg 52(4).

75 Itimu, Data Protection Commissioner Office Launches New Website and Logo, 2021.

76 ODPC Strategic Plan Financial Year 2022/23–2024/25.

77 ODPC, Vision, Mission and Core Values, https://www.odpc.go.ke/mandate-of-the-office/vision-mission-and-core-values/ (accessed 23 February 2022).

78 ODPC website, https://www.odpc.go.ke/ (accessed 8 August 2022). The decision to publish the reports is speculative only.

ducting a DPIA. The website is up to date, a step that is undoubtedly vital should the ODPC decide to publish DPIA reports on its website.

The Directorate of Data Protection Compliance is tasked with coordinating DPIAs in Kenya, carrying out inspections to ensure compliance with the requirements and reviewing and approving DPIAs done per section 31 of the Data Protection Act.[79] Also, the ODPC has established the Directorate of Research, Policy and Quality Assurance that coordinates development of guidelines and codes of practice for data controllers and processors.[80] The ODPC has also published a Guidance Note on Data Protection Impact Assessment,[81] which provides additional guidance materials, including a template for conducting DPIA.[82]

What stands out is the proactive approach that the Kenyan ODPC has adopted in executing its functions, including implementing the DPIA framework. This is a strategic and swift method of enforcing data protection rules and positions the ODPC as the 'gatekeeper of data protection compliance and enforcement'.[83]

2 Data Processor's Obligation to Conduct DPIA

Under Kenya's DPIA framework, the obligation to conduct a DPIA is not limited to the data controller.[84] A data processor[85] may also be required to conduct a DPIA.[86] The framing of section 31(1) of the Act is to the effect that either of the two can undertake a DPIA in respect of a data processing operation. This is slightly different from the language in the GDPR, which suggests that DPIA is a sole responsibility of a data controllers.[87]

---

79 ODPC, Directorates, https://www.odpc.go.ke/mandate-of-the-office/directorates/ (accessed 25 July 2022).

80 Data Protection Act 2019, s 74.

81 ODPC Guidance Note on DPIA.

82 This is in keeping with Data Protection (General) Regulations 2021, reg 50(1). The Regulation provides that the DPIA template under the Third Schedule to the Regulations is not final.

83 Paradigm Initiative and Babalola, *Data Protection Authorities in Africa Report* 2021, p. 7, https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-2.pdf (accessed 3 July 2023).

84 Under Data Protection Act 2019, s 2 a data controller on the other hand is a person who either alone or jointly with others determines the purpose and means of processing data. The word person here includes any natural or legal person, public authority, agency or other body.

85 Under Data Protection Act 2019, s 2 data processor is an entity which processes personal data on behalf of a data controller, while a data controller on the other hand is a person.

86 Data Protection Act 2019, s 31(1). This is similar to the approach under Mauritius Data Protection Act 2017, s 34(1).

87 GDPR Article 35(1).

Given this relationship, it is compelling to conclude that introducing the data processor's obligations in this regard ensures compliance to the best extent possible. However, this arrangement creates a challenge in determining who between the data controller and data processor has the primary obligation in a given case to conduct DPIA. It is more complicated where there are two or more entities involved. The Parliament apparently intended to avoid duplication when it used the word 'or' in section 31(1) of the Data Protection Act. Unfortunately, a lack of clarity could lead to a subsequent blame game to the detriment of data subjects. It is pivotal for the ODPC to issue guidance in determining who between the data controller and processor is to conduct DPIA in various circumstances.

3 Blacklist for DPIA Operations

Regulation 49(1) Data Protection (General) Regulations, read together with the ODPC Guidance Note on DPIA, provide categories of data processing operations that are considered to result in high risks to the rights and freedoms of a data subject and, therefore must be subjected to DPIA mandatorily.[88] They include: processing operations that utilise automated decision-making; processing of sensitive personal data; combining or linking data sets; processing of data using innovative solutions; large-scale data processing; and systematic monitoring of a publicly accessible area. These categories are common in blacklists in other jurisdictions.[89] Though there are slight differences when compared with other lists internationally, the remarkable similarities are important, especially regarding the efficiency of DPIA that may be conducted in cross-border data processing operations.

Some of the operations that appear in the blacklist are overlapping. For example, the processing of biometric and genetic data[90] are listed independently even though they fit into the broader category of processing sensitive personal data, which is also listed on the blacklist category.[91] Before the Regulations were adopted in 2021, Cabinet Secretary for ICT, Innovation and Youth Affairs was sued for failing to conduct a DPIA when rolling out a digital ID that involved the collection of biometric and genetic data.[92] The Court ordered the government to conduct a DPIA

88 *See* the Data Protection (General) Regulations 2021 and the ODPC's Guidance Note for a comprehensive view of data processing operations requiring a DPIA.

89 Balybina, What is and what isn't Subject to a DPIA under GDPR? An Update, 2020.

90 Data Protection (General) Regulations 2021, reg 49(1)(c).

91 Data Protection (General) Regulations 2021, reg 49(1)(e).

92 *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner* (Inter-

before fully implementing the digital ID system. When the Taskforce on the Development of Data Protection General Regulations adopted a black list, it was cognizant of the developments from the Court. The Taskforce listed processing of genetic and biometric data separately from the general category of processing of sensitive personal data. This was done ostensibly to demonstrate that the government had been appropriately guided by the norm that emerged from court judgments.

On the elasticity of the list, Regulation 49(1) Data Protection (General) Regulations 2021 notes that the blacklist is not exhaustive. The ODPC has the discretion to expand the list in the future. When the ODPC formulated its Guidance Note on DPIA, it did not expand the list provided in the Regulations. The Guidance Note has only consolidated the ten categories of blacklist operations in the Regulations into eight.[93]

4 Consideration of "Right as a Risk" in the DPIA Process

Kenyan Data Protection Act 2019 follows a risk-based approach in prescribing DPIA.[94] It considers a violation of human rights as a risk of which an assessment and mitigation must be undertaken in the DPIA process.[95] This is remarkable, especially when one considers that comparative national data protection law in Uganda does not provide for an assessment of risks to the rights and freedoms of data subjects as part of the DPIA process.[96] The Ugandan approach focuses only on traditional risks (usually categorised as physical, emotional and material).[97] The Kenyan approach, in contrast, has upscaled the risk assessment by enabling data controllers and data processors to assess the necessity and proportionality of data processing in relation to the purposes of the processing.[98] Van Dijk, Gellert, and Rommetveit note that the approach of assessment of risks to a right is more productive since it is based on a 'fair balance criterion' that guides person-

ested Party) (Judicial Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review) (14 October 2021) (Judgment) (*Ex-parte Katiba Institute & Another*).

93 ODPC Guidance Note on DPIA 2022, p. 8, https://www.odpc.go.ke/wp-content/uploads/2022/01/ODPC-guidance-note-on-Data-Protection-Impact-assessment.pdf (accessed 3 July 2023).

94 GDPR Art 35.

95 Data Protection Act 2019, s 31(2)(c).

96 Compare Kenyan Data Protection Act 2019, s 31(2)(c) with Ugandan Data Protection and Privacy Regulations 2021, reg 12(a)-(c).

97 Abu Dhabi Global Market Office of Data Protection Guidance on the Data Protection Regulations 2021, part 4.

98 Data Protection Act 2019, s 31(2)(b).

al data processing.[99] They also point out that this approach enables businesses to consider new technologies unsafe unless proven otherwise.

5 Meta-regulation, Self-Regulation and Emergence of Internal and Industry-Specific Regulations

Effective implementation of data protection in the digital age requires a meta-regulation approach. Meta-regulation is a form of regulation where the State regulates businesses by prescribing law, governance structures, and evaluation to ensure compliance.[100] In the Kenyan DPIA framework context, meta-regulation plays out in various ways. First, the legislature has passed Data Protection Act that prescribes DPIA. Second, the governance structure is designed so that the power to conduct DPIA rests on the data controllers and processors. These actors decide whether to undertake DPIA, deploy small-scale or large-scale DPIA, and put in place the technical and organisational requirements for conducting a DPIA, including appointment and designation of a data protection officer (DPO) where appropriate.

Third is the executive control or intervention by the regulator, in this case, the ODPC. In Kenya, the ODPC can intervene in the DPIA process to ensure control and compliance. The intervention is what Binns calls a 'triple loop of evaluation' that helps ascertain compliance.[101] The interventions may play out when data controllers or processors consult with the ODPC,[102] through submission of the DPIA report to the ODPC 60 days before the processing operation, and adherence to mandatory recommendations by the ODPC.[103]

Furthermore, Kenya's data protection framework complements meta-regulation with self-regulation. Particularly, the ODPC is tasked to 'promote self-regulation amongst data controllers and data processors'.[104] The principle of self-regulation envisages that the regulated entities shall take active and sustainable steps to monitor their adherence to the law. In the context of DPIA, this means that data controllers and processors can undertake sectoral data compliance measures. Already, the financial sector has taken the lead with a sectoral Data Privacy and Pro-

99 Dijk/Gellert/Rommetveit, *Comp and sec rev.* 2016, 2(32), p. 287.
100 Binns, *ID priv law* PL 2017, 22.
101 *Ibid,* p. 25.
102 Data Protection (General) Regulations 2021, reg 52.
103 Kenyan Data Protection Act 2019, s 31(5).
104 *Ibid,* s 8(1)(d).

tection Guidance Note to Kenya Digital Financial Services.[105] This sectoral Guidance Note complements the 2021 Regulations and the ODPC's Guidance Note on DPIA.

Another example is the emergence of the Central Bank of Kenya (CBK) as a co-regulator through the recently developed Central Bank of Kenya (Digital Credit Providers) Regulations.[106] The Regulations target previously unregulated digital credit providers and mandate them to develop independent assurance systems.[107] This means implementing appropriate policies[108] and safeguards[109] for the technologies used in digital lending.

6 Sufficiency of DPIA Template

The ODPC Guidance Note contains a six-page template of a DPIA report.[110] This template provides open-ended questions on the description of the processing operations, assessment and proportionality of the processing operations, assessment of risks to rights and freedoms of data subjects, risk mitigation measures, sign-off and record of outcomes. The Data Protection (General) Regulations 2021 complement the assessment questions to be filled out in five sections.[111] The open-ended questions in the DPIA templates provide an avenue for robust assessment and review by ODPC.

However, the templates exclude sections on record of engagements with stakeholders in the DPIA process whenever necessary. As it is, data controllers and processors can identify risks and risk mitigation mechanisms independently without additional inputs from involved stakeholders. Since the design does not prioritize engagement of data subjects or other relevant stakeholders, it can possibly be used by data controllers without explanation and transparency.[112] This may be more concerning, especially when the Kenyan government partners with foreign compa-

105 Financial Services Deepening (FSD) Kenya, *Data Privacy and Protection: Guidance Note to Kenya Digital Financial Services*, https://www.fsdkenya.org/wp-content/uploads/2021/08/DAPA-Report-08272021.pdf (accessed 6 February 2022).

106 Central Bank of Kenya (Digital Credit Providers) Regulations 2022.

107 *Ibid*, reg 4(3)(f).

108 *Ibid*, reg 13.

109 *Ibid*, reg 15(3).

110 ODPC Guidance Note on DPIA 2022.

111 The Data Protection (General) Regulations 2021, Third Schedule.

112 That is so because the lack of stakeholder engagement may render the data controller or data processor unable to: identify risks to the rights and freedoms, appreciate their impact and identify mitigation measures.

nies to implement new technologies. Considering its importance, the ODPC should develop some guidance on stakeholder engagement.[113]

7 Reporting and Publication of a DPIA Report

A DPIA is an organisational measure for compliance, accountability, and transparency. Transparency is essential because DPIA can snowball into a box-ticking exercise without scrutinising a DPIA report, much to a disservice to data subjects. On the one hand, it is comforting to note that the data protection law in Kenya gives the ODPC opportunity to review DPIA reports developed by data controllers and processors.[114] Upon review, the ODPC has two options. First, it may approve the report expressly keep silent for 60 days. Second, it may provide binding recommendations. In case of binding recommendations, the data controller is to resubmit a reviewed or revised DPIA report. This mechanism of review provides an element of transparency and protection to data subjects.

On the other hand, since data controllers and processors are not required to publicise the DPIA reports, there is no total transparency to the general public. First, although the Access to Information Act 2016 provides means by which the data subjects can request access to the DPIA report, there could be challenges for data controllers or data processors to yield to a request for access to information in circumstances when the DPIA report contains sensitive personal data, for example.[115] Second, several exceptions to the right of access to information[116] may hinder any attempt of a third-party scrutiny.

8 Court as an Instrumental Norm Developer

Kenya has had some remarkable practical and judicial experiences with high-risk processing of personal data before and after the enactment of the Data Protection Act 2019. Notably, courts have been called to consider myriad concerns arising from government plans for digital migration, a program by Equity bank to deploy thin sim technology,[117] and plans by the Communications Authority of Kenya (CA) to roll out the implementation of device management system (DMS) into the net-

113 Mukherjee et al., *Int. j. innov. re. technolog. sci. eng, Jour. IRSET* 2019, p. 12.
114 Data Protection Act 2019, s 31(5).
115 *Ibid*, s 31(6) provides basis for the guidelines.
116 Access to Information Act 2016, ss 6 and 9.
117 *Bernard Murage v Fineserve Africa Limited & 3 others* [2015] eKLR.

works of the telecommunication operators in Kenya.[118] The most recent concerns emanated from the government's plan to implement the national integrated identity management system, which would require issuing digital ID to citizens and foreign residents in Kenya.[119]

In deciding these issues, the High Court played a crucial role in shaping the course of data governance in Kenya.[120] This is evident considering how the jurisprudence developed by the High Court has informed the subsequent high risk processing of personal data in digital revenue collection systems and biometric registration of members of political parties and voters.

More recently, in a landmark decision the High Court made a ground-breaking ruling that the requirement to conduct a DPIA derives from the constitutionally guaranteed right to privacy.[121] This case arose from complaints that the government's plan to implement a digital ID[122] was intrusive and breached privacy and data protection. The case was petitioned by the Nubian Rights Forum and other persons at the High Court. The argument was that this process involved the collection of DNA and the GPS location of citizens and foreign residents.[123] Eventually, the Court ruled that the government should conduct a DPIA before embarking on the plan, given its high-risk processing.[124]

When the government showed intention to proceed in disregard of the Court order, Katiba Institute, a non-governmental organisation, filed the judicial review before the Court.[125] Katiba Institute argued, among others, that the requirement to conduct DPIA under section 31 of the Data Protection Act 2019 applied retrospectively to the government's plan to roll out a digital ID system. In the end, the

118 *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others* [2018] eKLR.

119 *Nubian Rights Forum & 2 others v Attorney-General & 6 others; Child Welfare Society & 8 others (Interested Parties); Centre for Intellectual Property & Information Technology (Proposed Amicus Curiae)* [2019] eKLR (*Nubian Rights Forum & 2 others v Attorney-General*).

120 *Ex-parte Katiba Institute & Another Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested Party)* (Judicial Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review) (14 October 2021) (Judgment) (*Ex-parte Katiba Institute & Another*).

121 *Nubian Rights Forum & 2 others v Attorney-General.*

122 This was to be done vide an amendment to the Registration of Persons Act cap 107 Laws of Kenya through a Statute Law (Miscellaneous Amendments) Act 2018.

123 *Nubian Rights Forum & 2 others v Attorney-General,* paras 27, 57, 58 and 100.

124 *Nubian Rights Forum & 2 others v Attorney-General.*

125 *Ex-parte Katiba Institute & Another.*

Court found that the government is obligated to conduct a DPIA whether or not the enabling data protection law is in force.[126]

The Court developed an important norm by deciding that the obligation to conduct a DPIA is a derivative of Article 31 of the Constitution.[127] In effect, the Court has set a rule that data subjects cannot be prejudiced by the data controller's or processor's failure to conduct a DPIA due to the lack of enabling legislation.[128]

It seems that this is the first time in Africa that a judicial review court took a human rights approach to DPIA and decided for a retrospective application of an obligation to conduct DPIA. Under the approach, DPIA should be seen as one of the envisaged safeguard measures necessary to protect the right to privacy fully and effectively. The jurisprudence promotes fairness on the part of data subjects. It sets the ground for interpreting the State's international human rights duty to protect, respect and promote human rights for more robust protection of data subjects.

Otieno has separately argued that the case mentioned above has considerable potential to influence norm development in Kenya and the African region.[129] Governments of African States without data protection laws may no longer hide behind the shield of lack of data protection law to fail to conduct or support the DPIA exercise for high-risk data processing activities. Other nations should emulate such a progressive decision in developing other areas of human rights that require due diligence mechanisms for better protection of African citizens.

E Key Lessons and Recommendations for the African Region

The preceding discussion identified essential aspects of conducting DPIA. These aspects illustrate the need or importance of adopting DPIA in Africa at the regional, sub-regional and national levels. Below, these lessons are summarised.

126 *Ex-parte Katiba Institute & Another*, para 15.

127 *Ibid*, para 73.

128 *Ibid*, paras 96 and 99.

129 Otieno, 'Good order as Basis for Conducting Data Protection Impact Assessment during Transitional Periods, 2022, https://africanlegalstudies.blog/2022/01/21/good-order-as-basis-for-conducting-data-protection-impact-assessment-during-transitional-periods/ (accessed 1 July 2023).

I Legal reforms in subsequent African regional and sub-regional instruments should include DPIA provisions to bring the region at par with other regions

There seems to be a global trend to introduce a proactive risk-based approach in data protection, and several reforms occurring after the adoption of the GDPR indicate this. For example, the modified Convention 108+ requires parties to include DPIA in their framework. Undoubtedly, practical benefits have been recorded, as highlighted in the Dutch examples discussed earlier. The importance attached to DPIA by the Kenyan High Court is also a testament to the value of this tool. As already stated, the Court emphasized that DPIA is an inherent and mandatory constitutional means for ensuring the right to privacy, and this requirement is indispensable.[130]

Therefore, it is recommended that any subsequent amendments to the African regional and sub-regional instruments on data protection should include a risk-based approach and a DPIA mechanism. This should also extend to new instruments developed at regional, sub-regional and State levels. While these reforms are expected, organisation are encouraged to adopt DPIA in their internal rules. It is commendable that professional rules such as the IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa 2021 recognise this tool. Such should be emulated by others. Courts across the continent are also encouraged to promote risk-based approach and enforce DPIA as a compliance mechanism.

II Data Protection Authorities in Africa would benefit from the proactive use of the DPIA tool

One of the avenues of reaping the benefits of DPIA is to use it as a proactive tool in the hands of the data protection authorities. This forces data controllers and processor to incorporate privacy by design at all levels, an architecture contemplated in most of the African national data protection laws. However, the reality shows that organisations are largely unwilling to deploy DPIA proactively in some cases, including the example from the Kenyan digital ID case.[131] To discourage

130 *Ex-parte Katiba Institute and Another*, para 15.

131 There are also concerns that Kenya's Independent Electoral and Boundaries Commission may not have conducted a DPIA in respect of the electronic voting system it deployed in the conduct of the 2022 general elections. While the concerns may have not been verified, they only go far in sup-

such attitudes, it is recommended that African data protection authorities should be proactive in enforcing the requirement of DPIA. This they can do by initiating investigations *suo moto* against entities that fail to comply with the rules, especially in high-impact personal data processing operations such as national identification schemes.

Again, taking a cue from the Dutch examples and other parts of Europe, authorities in Africa should strive to proactively uncover data protection risks in ongoing projects, especially in high-impact personal data processing operations or projects such as banking, election systems, national identification systems, etc. A DPIA is a valuable tool to deploy in this respect before the risks materialize.

III Africa can harness DPIA developments to its advantage

As African States gear towards developing their DPIA frameworks, there are obvious opportunities for improvement, while reflecting the African unique approach to privacy and data protection contexts. These States can leverage existing regulatory advances made in other regions and by professional bodies to enhance their frameworks. For example, the International Organization for Standardization (ISO) has published several standards on risk management such as ISO 31000:2018 on risk management,[132] and ISO 29134:2017 guidelines for conducting DPIA.[133] The National Institute of Standards and Technology (NIST) also has some useful guidance for information security risk management, including NIST Special Publication (SP) 800–30, Guide for Conducting Risk Assessments.[134]

Besides international standards, there are opportunities for cross-pollination of international best practices documented in DPIA guidelines developed by other data protection authorities. Some of the notable authorities whose guidelines could be useful for African States' DPIA frameworks include the European Data Protection Board,[135] the UK's ICO,[136] the French CNIL,[137] the Spanish AEPD,[138]

porting why such frameworks must focus on requiring data controllers and processors to take proactive steps in assessing the need for DPIA.

132 The ISO 1000:2018 Risk management is an updated version of the 2009 guidelines.

133 ISO 29134:2017, pp. 4–30.

134 NIST SP 800–30, https://www.nist.gov/privacy-framework/nist-sp-800-30 (accessed 17 November 2022).

135 See EDPB, *Opinions,* https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en (accessed 15 November 2022).

136 ICO, *supra* n. 4.

137 CNIL, *Privacy Impact Assessment,* https://www.cnil.fr/en/privacy-impact-assessment-pia (accessed 12 November 2022).

among others. While these guidelines have some notable variances, they could enrich adopting States and take the advantage of the possibilities they offer to customise their frameworks.

Lastly, African States stand at a vantage position given there has been considerable research on the topic of DPIA. The existing research offers Africa the opportunity for improvement. Examples of these research sources include the NIST's works on privacy engineering and risk management;[139] the book titled *Privacy Impact Assessment* edited by Wright and Hert;[140] and a host of other academic publications.[141] In sum, African States can utilise these sources to design DPIA frameworks that work for the African specific contexts.

F Conclusion

DPIA is a recent tool for compliance and accountability. Unlike the EU where GDPR prescribes DPIA at the Union level, this mechanism is not seen in key African regional and sub-regional frameworks on data protection. This research has shown the trends in the adoption of DPIA at the national levels in Africa, revealing several approaches among African States. While some countries do not provide for it at all, others provide for it albeit with varying compliance thresholds and requirements. Despite the variances, African States are increasingly adopting the DPIA mechanism in the high-risk personal data processing.

The DPIA framework in Kenya has been examined in this work, noting the prospects and challenges in the framework. Remarkably, the Kenyan ODPC swung into action after its inauguration, including developing Guidance Notes on DPIA and resolution of complaints. All these have helped to progressively cultivate the culture of compliance with DPIA requirements.[142] Other factors too have boosted the implementation of DPIA in Kenya including the express provision of the obligation in the principal legislation on data protection; comprehensive black-

138 AEPD, Gestión Del Riesgo y Evaluación De Impacto En Tratamientos De Datos Personales 2021, https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf (accessed 12 November 2022).

139 Sean Brooks et al, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, US Department of Commerce, National Institute of Standards and Technology, 2017, p. 1.

140 Wright/De Hert (eds) *Privacy Impact Assessment*, Springer 2012, 3 (32).

141 Nwankwo, *supra.*

142 Already, the Kenya National Government's Ministry of ICT and Youth Affairs conducted DPIA on Huduma Namba. Stima Sacco and Kenya Power and Lighting Company also kick-started the processes of conducting DPIA under the new law.

list and whitelist; judicial pronouncement on the subject matter and statutory anchoring on self-regulation.

In the end, three key lessons have been learned towards adopting the DPIA mechanisms at all levels in Africa, including the need for legal reforms at the regional and sub-regional levels to incorporate a risk-based approach and DPIA tool; the need for data protection authorities to optimise their powers by encouraging proactive use of DPIA, which will improve self-regulation; and lastly, African States stand at a vantage position in designing their DPIA frameworks since they do not start on a blank slate. They could harness existing DPIA mechanisms, of which an array of international standards, national guidelines and academic publications have been identified in this work. African stakeholders can rely upon these to develop their unique DPIA frameworks.

G Bibliography

Abu Dhabi Global Market Office of Data Protection Guidance on the Data Protection Regulations 2021.

AEPD, GUÍA para una Evaluación de Impacto en la de Protección Datos Personales 2014 <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf> (accessed 12 May 2019).

AEPD, Gestión Del Riesgo y Evaluación De Impacto En Tratamientos De Datos Personales 2021 <https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf> (accessed 12 November 2021).

AEPD, *GDPR Risk Assessment* <https://evalua-riesgo.aepd.es/index_en.html> (accessed 15 November 2022).

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

African Declaration on Internet Rights and Freedoms 2014 <https://africaninternetrights.org/> (accessed 14 November 2022).

AU Digital Transformation Strategy for Africa 2020–2030 <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf> (accessed 14 November 2022).

Boshe/Hennemann, *Data Protection Laws in Northern Africa – Regulatory Approaches, Key Principles, Selected Instruments*, Konrad-Adenauer-Stiftung e.V. 2022.

Bhargava, The Shifting Data Protection Paradigm: Proactive vs. Reactive (25 July 2017) https://devops.com/shifting-data-protection-paradigm-proactive-vs-reactive/ (accessed 18 March 2019).

Binns, Data Protection Impact Assessments: A Meta-Regulatory Approach, *ID priv. law, Vol. 7 (1), 2017*, p. 22–35.

Borocz, Risk to the Right to the Protection of Personal Data: An Analysis through the Lenses of Hermagoras *EDP law rev. 2(4), 2016, p. 467–480.*

Bock *et al*, Data Protection Impact Assessment for the Corona App, 2020 <https://www.fiff.de/dsfa-corona-file-en/at_download/FIfF-CoronaApp-DSFA-EN-v1.6.pdf> (accessed 8 November 2022).

Brooks *et al*, An Introduction to Privacy Engineering and Risk Management in Federal Systems, 2017 <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf> (accessed 6 November 2022).

Balybina, What is and what isn't Subject to a DPIA under GDPR?: An Update, 2020 <https://iapp.org/news/a/what-is-and-what-isnt-subject-to-a-dpia-under-gdpr-an-update/> (accessed 4 August 2022).

BSI, 'Technical Guidelines RFID as Templates for the PIA-Framework, 2010 <bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_RFID_-Templates_for_PIA_Framework_pdf.pdf?__blob=publicationFile&v=1> (accessed 12 January 2020).

Centre for Information Policy Leadership, A Risk-based Approach to Privacy: Improving Effectiveness in Practice, 2014 <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf> (accessed 12 January 2020).

Central Bank of Kenya (Digital Credit Providers) Regulations 2022.

Clarke, Privacy Impact Assessment: Its Origins and Development, 25 *Comp and sec rev.* 2, Vol. 25, 2009, p. 123–135.

CNIL, Methodology for Privacy Risk Management – How to Implement the Data Protection Act (June 2012) <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf> (accessed 12 May 2019).

CNIL, *The Open Source PIA Software Helps to Carry Out Data Protection Impact Assessment* 2021 <https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assessment> (accessed 15 November 2022).

CNIL, Privacy Impact Assessment (PIA) <https://www.cnil.fr/en/privacy-impact-assessment-pia> (accessed 12 November 2022).

Chart of Signatures and Ratifications of Treaty 108 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108> (accessed 15 November 2022).

Chart of Signatures and Ratifications of Treaty 223 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223> (accessed 15 November 2022).

Convention 108 + Convention for the Protection of Individuals with Regard to the Processing of Personal Data <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf> (accessed 15 November 2022).

Demetzou, in: Kosta et al (eds), *Privacy and Identity Management Fairness, Accountability and Transparency in the Age of Big Data*, Springer International Publishing 2019.

Demetzou, Data Protection Impact Assessment: A Tool for Accountability and the Unclarified Concept of 'High Risk' in the General Data Protection Regulation *35(6) Comp. and sec. rev.*,2019.

Dijk/Gellert/Rommetveit, A Risk to A Right? Beyond Data Protection Risk Assessments, 32 *Comp. and sec. rev.* 2016 (2).

Data Protection (General) Regulations 2021.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.

Declaration of Principles on Freedom of Expression and Access to Information in Africa (Adopted by the African Commission on Human and Peoples' Rights at its 65th Ordinary Session held from 21 October to 10 November 2019 in Banjul, the Gambia).

European Commission Recommendation of 12 May 2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification (OJ L 122/47).

European Commission, A Comprehensive Approach on Personal Data Protection in the European Union COM (2010) 609 final.

European Commission, 'Data Protection Impact Assessment for Smart Grid and Smart

Metering Environment' <https://ec.europa.eu/energy/topics/markets-and-consumers/smart-grids-and-meters/smart-grids-task-force/data-protection-impact-assessment-smart-grid-and-smart-metering-environment_en> (accessed 12 January 2020).

European Data Protection Board, 'Opinions' <https://edpb.europa.eu/our-work-tools/consistency-findings/opinions_en> (accessed 24 December 2019).

Friedewald et al., Data Protection Impact Assessment in Practice *Computer Security ESORICS 2021 International Workshops, Volume 13106* (2022) <https://link.springer.com/chapter/10.1007/978-3-030-95484-0_25> (accessed 15 November 2022).

Fisheries and Oceans Canada, Access to Information and Privacy (ATIP) Procedure Manual, p. 52 < https://waves-vagues.dfo-mpo.gc.ca/library-bibliotheque/277874.pdf > (accessed 1 July March 2023.

Flaherty, Privacy Impact Assessments: An Essential Tool for Data Protection. *A presentation to a plenary session on 'New Technologies, Security and Freedom', 22nd Annual Meeting of Privacy and Data Protection Officials, Venice, September 27–30, 2000* <https://aspe.hhs.gov/legacy-page/privacy-impact-assessments-essential-tool-data-protection-142721> accessed 8 July 2019.

Financial Services Deepening (FSD) Kenya, 'Data Privacy and Protection: Guidance Note to Kenya Digital Financial Services' < https://www.fsdkenya.org/wp-content/uploads/2021/08/DAPA-Report-08272021.pdf> (accessed 6 February 2022).

Greenleaf/Cottier, International and Regional Commitments in African Data Privacy Laws: A Comparative Analysis, CLSR 1, Vol 44,2022.

ICO, PIA Handbook 2007 (version 1.0, December 2007), as revised in 2009.

ICO, 'Data Protection Impact Assessments' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/> (accessed 2 February 2022).

Itimu, Data Protection Commissioner Office Launches New Website and Logo <https://techweez.com/2021/02/25/data-protection-commissioner-office-new-website-logo/> (accessed 25 July 2022).

ISO 22307: 2008 Financial Services – Privacy Impact Assessment (ISO 2008).

ISO/IEC 29134:2017 Information technology – Security techniques – Guidelines for Privacy Impact Assessment.

ISO 31000:2018 Risk Management – Guidelines.

IBA, IBA African Regional Forum Data Protection/Privacy Guide for Lawyers in Africa (2021).

Judicature Act 1967.

Kuner et al, Risk Management in Data Protection 5 (2) IDPL 96 (2015).

Kenyan Constitution 2010.

Kenya Information and Communications (Consumer Protection) Regulations 2010.

Kenya Data Protection Bill 2012.

Kenya Privacy and Data Protection Policy 2018.

Kenya Data Protection Bill 2019.

Kenyan Data Protection Act 2019.

Kenya Access to Information Act 2016.

Linden Consulting Inc, Privacy Impact Assessments: International Study of their Applications and Effects (October 2007).

Mauritius Data Protection Act 2017.

Mukherjee *et al.,* How Stakeholder Engagement Affects IT Projects (March 16, 2019) <http://dx.doi.org/10.2139/ssrn.3415959> (accessed 17 February 2022).

Nwankwo, Towards a Transparent and Systematic Approach to Conducting Risk

Assessment Under Article 35 of the GDPR (PhD Thesis 2021) <https://www.repo.uni-hannover.de/handle/123456789/11451> (accessed 10 October 2022).

Nwankwo, The "Whitelist" and its Value during a Data Protection Impact Assessment in: *Turning Point in Data Protection Law*, (2020) 141<https://dpoblog.eu/the-whitelist-and-its-value-during-a-data-protection-impact-assessment> (accessed 10 October 2022).

NIST SP 800–30, <https://www.nist.gov/privacy-framework/nist-sp-800-30> (accessed 17 November 2022).

Nigeria Data Protection Bill 2022, <https://ndpb.gov.ng/Files/Nigeria_Data_Protection_Bill.pdf> (accessed 17 November 2022).

Namibia Draft Data Protection Bill 2022, <https://mict.gov.na/documents/32978/1376285/Data+Protection+Draft+Bill++March+2022....pdf/7c91ff30-2ec4-4ed2-99de-e09ac46466d8> (accessed 12 November 2022).

Ollivier, Ivory Coast – Data Protection Overview (January 2022) <https://www.dataguidance.com/notes/ivory-coast-data-protection-overview> (accessed 17 November 2022).

ODPC, Strategic Plan Financial Year 2022/23–2024/25' <https://www.odpc.go.ke/wp-content/uploads/2021/06/ODPC-Strategic-Plan.pdf> (accessed 23 February 2022).

ODPC, Vision, Mission and Core Values <https://www.odpc.go.ke/mandate-of-the-office/vision-mission-and-core-values/> (accessed 23 February 2022).

ODPC Website <https://www.odpc.go.ke/> (accessed 8 August 2022).

ODPC, Directorates <https://www.odpc.go.ke/mandate-of-the-office/directorates/> (accessed 25 July 2022).

ODPC Guidance Note on DPIA.

Otieno, 'Good order' as Basis for Conducting Data Protection Impact Assessment during

Transitional Periods <https://africanlegalstudies.blog/2022/01/21/good-order-as-basis-for-conducting-data-protection-impact-assessment-during-transitional-periods/> (accessed 15 July 2022).

Personal Data Protection Guidelines for Africa 2018.

Privacy Company, DPIA Diagnostic Data in Microsoft Office Proplus (5 November 2018).

PAK & another v Attorney General & 3 others (Constitutional Petition E009 of 2020) [2022]

KEHC 262 (KLR) (24 March 2022) (Judgment)'.

Paradigm Initiative and Babalola, 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 <https://paradigmhq.org/wp-content/uploads/2021/09/DPA-Report-2.pdf> (accessed 17 October 2022).

Renn *et al*, *Precautionary Risk Appraisal and Management: An Orientation for Meeting the Precautionary Principle in the European Union,* Europäischer-hochschulverlag 2009.

Roe v Wade 410 U.S 113 <https://supreme.justia.com/cases/federal/us/410/113/> (accessed 8 November 2022).

Rijksoverheid, Data Protection Impact Assessments DPIA's Office 365 ProPlus, Windows 10 Enterprise, Office 365 Online and Mobile Apps, 2019 <https://www.rijksoverheid.nl/documenten/rapporten/2019/06/11/data-protection-impact-assessment-windows-10-enterprise> (accessed 1 July 2023).

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 (OJ L 119, 4.5.2016).

Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Exparte); Immaculate Kasait, Data Commissioner (Interested

Party) (Judicial Review Application E1138 of 2020) [2021] KEHC 122 (KLR) (Judicial Review) (14 October 2021) (Judgment) (*Ex-parte Katiba Institute & Another*).

Registration of Persons Act cap 107 Laws of Kenya.

Statute Law (Miscellaneous Amendments) Act 2018.

Som/Hilty/Köhler, The Precautionary Principle as a Framework for a Sustainable Information Society, 85 *J. of Buss. Eth.* (2009) 493.

Rijk, DPIA Google G Suite Enterprise (updated 12 February 2021) <https://open.overheid.nl/repository/ronl-c3f769fa-0c07-4df9-944e-f70c52f53bf4/1/pdf/Google%20Workspace%20DPIA%20for%20Dutch%20DPA%2012%20Feb%202021.pdf> (accessed 17 November 2022).

Speed, *Dutch public sector gets green light to use Google Workspace* (2022) https://www.theregister.com/2022/05/30/google_workspace_dutch_government/ (accessed 17 November 2022).

Tancock/Pearson/Charlesworth, The Emergence of Privacy Impact Assessments *HP Laboratories HPL-2010–63*, 10 <http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf> (accessed 2 July 2023.

The Departmental Communication, Information and Innovation, Report on the Consideration of the Data Protection Bill, 2019 (October 2019) <http://www.parliament.go.ke/sites/default/files/2019-10/Report%20on%20Data%20Protection%20Bill%2C%202019_compressed.pdf> (accessed 22 February 2022) (Report on the Consideration of the Data Protection Bill, 2019).

Ugandan Data Protection and Privacy Regulations 2021.

Wright et al, A Privacy Impact Assessment Framework for Data Protection and Privacy Rights (Prepared for the European Commission Directorate General Justice JLS/2009–2010/DAP/AG, 21 September 2011) <https://biblio.ugent.be/publication/8738598> (accessed 15 November 2022).

Wright et al, 'Precaution and Privacy Impact Assessment as Modes Towards Risk Governance, in: *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publications Office of the European Union, 2011.

Wright/De Hert (eds), *Privacy Impact Assessment* Springer 2012.

Setor Foe-Ahorney

Does the Law Protect the Privacy of Ghanaians on the Internet? An Exploratory Study

A Introduction

From 1995, when Ghana first had full access to the internet[1] to-date, the country has made some significant strides in internet penetration. It was among the first African countries to reform its ICT sector and liberalise telecommunication with active private sector provision of services. Experts have estimated the ICT sector to be valued at about $1 billion. This value may reach $5 billion by 2030.[2] At present, the country can boast of over 16,9 million users of the internet (as of February 2022), a penetration rate of 53 %[3] for its total population of over 32,2 million people.[4] While this rate represents a huge leap in internet usage over previous

1 Acheampong, The State of Information and Communication Technology and Health Informatics in Ghana, *OJPHI* 4(2):4191, 2012, p 4.

2 Ghana – Country Commercial Guide, https://www.trade.gov/country-commercial-guides/ghana-information-and-communications-technology-ict (accessed 27 July 2022).

3 Kemp, Digital 2022: Ghana, https://datareportal.com/reports/digital-2022-ghana (accessed 27 June 2022).

4 Ghana Population Clock, https://t.ly/u9aXB (accessed 27 June 2022).

https://doi.org/10.1515/9783110797909-008

years[5] (a 49,1% growth from 2000 to 2021)[6], Ghana still lags behind the global average of 63,1%.[7] Nonetheless, internet usage in Ghana is the highest in the West African sub-region and the 13th in the whole of Africa.[8]

This recent surge in internet usage has been a result of a number of factors including government policies pushing for digitization and digitalization of the economy, expansion in broadband and other digital infrastructure, new development in ICT, proliferation of fintech companies and the increased use of smartphones and social media. All these have brought unique opportunities including reforming the criminal justice system,[9] e-commerce and e-banking,[10] e-government services,[11] social media and mobile phones products and services. Ghana's ICT Policy for Accelerated Development (ICT4AD) adopted in 2004 is the blueprint for digital transformation in the country. Other policies driving ICT development in the country includes the National Telecommunication Policy (NTP),[12] National Science Technology and Innovation (STI) Policy,[13] and the National Broadband Policy and Implementation Strategy.[14] There are also several government initiatives that are promoting the use of internet in Ghana. The initiatives include the collaboration between the Ministry of Communications and Digitalisation, the Ministry of

5 Quarshie and Ami-Narh, The Growth and Usage of Internet in Ghana, *JETCIS* 3(9):1302–1308, 2012, p 1303.

6 Percentage change in internet usage in West Africa between 2000 and 2021, by country, https://t.ly/CLK9 (accessed 01 August 2022).

7 Global internet penetration rate as of July 2022, by region, https://t.ly/MBuy (accessed 01 August 2022).

8 Share of internet users in Africa as of January 2022, by country, https://t.ly/Fkgt (accessed 01 August 2022).

9 Ouassini and Amini, Cybersecurity in Ghana, past, future and the present, in: Romaniuk and Manjikian (eds), Routledge Companion to Global Cyber-Security Strategy, p 1.

10 Digital Financial Services Policy, https://mofep.gov.gh/sites/default/files/acts/Ghana_DFS_Policy.pdf (accessed 01 August 2022).

11 Ghana e-Government Interoperability Framework, https://nita.gov.gh/theevooc/2017/12/Ghana-eGovernment-Interoperability-Framewo rk.pdf (accessed 01 August 2022).

12 National Telecommunications Policy, 2005, https://www.researchictafrica.net/countries/ghana/National_Telecommunications_Policy_ 20 05.pdf (assessed 01 August 2022).

13 National Science Technology and Innovation (STI) Policy, 2010, http://www.ecowrex.org/system/files/repository/2010_national-science-technology-and-innovation-policy_m.e.s.t.-ghana.pdf (accessed 01 August 2022).

14 National Broadband Policy and Implementation Strategy, 2012, https://nca.org.gh/wp-content/uploads/2020/09/National-Broadband-Policy-and-Implementation-Strategy.pdf (accessed 01 August 2022).

Education and Huawei Technologies to train 100,000 senior high school girls in cyber security and data privacy in several regions of Ghana.[15]

The high internet usage in Ghana can also be explained by the increased usage of mobile phones in the country. There are an estimated 44 million unique cellular phone connections in the country with 91,9 % of users accessing the internet via mobile phones and spending an average of four and half hours daily using mobile internet. Most Ghanaian mobile phone users have two phones and typically use SIM cards from different mobile networks. There are also 8,80 million active social media users in the country who would usually access their accounts on smartphones.[16]

A rise in internet penetration has its shortcoming as well. It gives cybercriminals greater opportunity to engage in illegal activities, providing them with a large number of potential victims that they can effectively and efficiently engage. It is recorded that globally, victims of cybercrime lose an estimated amount of $318 billion annually.[17] In Ghana, $114,8 million was lost to cybercrime in the years of 2018 and 2019.[18] Ghana was ranked second after Nigeria in the top 5 cybercrime offending countries in Africa.[19] It is therefore not surprising that "sakawa", a term frequently used to depict internet fraud originated from Ghana, being added to the lexicon on cybercrime in the region.

Ghana has made some remarkable strides in the fight against cybercrime. It has reviewed its national cybersecurity policy and strategy, has enacted a cybersecurity law to complement the existing laws such as Data Protection Act, 2012 (Act 843) and the Electronic Transactions Act, 2008 (Act 772). Ghana has also signed up to some international conventions and treaties[20] to help with the fight against cybercrime. These are the Convention on Cybercrime (Budapest Convention),[21] the

15 100,000 Girls Targeted for This Year's Girls-In-ICT (SHS) Training in Cyber Security and Data Privacy, https://t.ly/0t0j (accessed 01 August 2022).

16 Ibid n (3).

17 Cybercrime victims lose an estimated $318 billion annually, https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/ (accessed 01 August 2022).

18 Ghana loses more than $114 m to cybercrime in two years, https://t.ly/ymFr (accessed 3 November 2022).

19 5 African countries with the most Internet scammers, https://businesselitesafrica.com/2022/06/29/top-5-african-countries-with-the-most-internet-scammers/ (accessed 01 August 2022).

20 Ghana ranked third in Africa on Global Cybersecurity Index, https://t.ly/HKzWF (accessed 19 July 2022).

21 Convention on Cybercrime, https://rm.coe.int/1680081561 (accessed 01 August 2022).

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)[22] and the ECOWAS Regional Critical Infrastructure Protection Policy.[23]

B Cyber Threat Landscape in Ghana

Internet users in Ghana mostly fall victim to phishing, traditional cybercriminal activities (identity theft, credit card fraud, email scams, and mobile money frauds), child pornography, simbox fraud/interconnect bypass fraud, malware and botnets attacks, hacking and data breaches. The Ghana Police Service Cyber Crime Unit identified six cyber offences that are prevalent in Ghana.[24] These six offences are hacking, internet fraud, identity theft, phishing, internet extortion and child exploitation. A study conducted by the FBI in 2013 showed that Ghana ranked second after Nigeria among the top cybercrime-offending countries in Africa and the sub region.[25] Between 2016 and 2018, Ghana lost an approximate amount of USD 230 million to cybercrime cases with more than half of the reported cases being linked to fraud.[26] By 2020, a year after the Cybercrime Incident Reporting Points of Contact was launched (in October 2019), the number of reported cases had skyrocketed to a total of 11,000 cybercrime cases.[27]

I Motivation for Cybercrimes in Ghana

The perpetrators behind cybercrime within the Ghanaian cyber space remain both foreign nationals and Ghanaians (e. g., insiders in an organization, laptop and mobile phones repairers). The motivation for cybercrime or the root causes for the

22 African Union Convention on Cyber Security and Personal Data Protection, https://t.ly/qkkp (accessed 01 September 2022).
23 ECOWAS Regional Critical Infrastructure Protection Policy, https://t.ly/NMMAj (accessed 01 September 2022).
24 Ghana Police Service Cyber Crime Unit, https://police.gov.gh/en/index.php/cyber-crime (accessed 01 September 2022).
25 Ibid fn 19.
26 Ghana loses $230 m to cyber criminals – CID, https://t.ly/7hlX (accessed 01 September 2022).
27 Ghana records over 11,000 cybercrime cases since 2019, https://www.graphic.com.gh/news/general-news/ghana-records-over-11-000-cybercrime-cases-in-a-year.html (accessed 01 September 2022).

increase in cybercrime in Ghana remains poverty, corruption, minimal regulatory frameworks, and unemployment.[28]

Many people in Ghana are persistently poor. Around 3.5 million people live in extreme poverty on less than $1.90 a day, majority of them in rural areas.[29] In 2021, about 13,4 % of the economically active labour force were unemployed.[30] In the same year, Ghana was ranked 73 (out of 180) on the Corruption Perception Index.[31] All of the above-mentioned facts have contributed to conditions that are actively driving many Ghanaians, especially the youth into cybercriminal activities. The Sakawa culture where criminals, who obtain a lot of wealth through cyber fraud, engage in opulence and display lavish lifestyles is also an attracting factor for the youth to get involved in cybercrime[32].

The menace of cybercrime also persists due to the lack of or minimal awareness on cybersecurity. Not many sensitization programmes exist to educate the ordinary Ghanaian on the dangers that the internet poses to them and how they can minimize their exposure to such threats.[33] There is also the lack of culture in reporting cyber breaches, reasons being that such a person does not know the channel through which to report or has not identified the need or essence of reporting. Not many Ghanaians are aware that the month of October is the cybersecurity month[34] and not so many Ghanaians are aware of the reporting system put in place by the National Cyber Security Authority. Not many Ghanaians are aware of the cybercrimes that takes place within the cyber ecosystem in Ghana. Majority of Ghanaians are only aware of mobile money scam and the National Lottery Authority (NLA) scam.

Also, part of the reasons why cybercrime is still prevalent in the country is the outmoded legislation, for example, the Evidence Act 1975 (NRCD 323) and the Criminal and other Offences Act, 1960 (Act 29) which were enacted before Ghana first made contact with the internet. These major enactments that were mostly used in

28 Baylon and Antwi-Boasiako, Increasing internet connectivity while combating cybercrime: Ghana as a case study, Centre for International Governance Innovation and Chatham House Paper Series: NO. 44, 2016, https://t.ly/3zlN (accessed 01 September 2022).

29 Number of people living in extreme poverty in Ghana from 2016 to 2022, by area, https://t.ly/KBhR (accessed 01 September 2022).

30 Ghana 2021 Population and Housing Census, General Report Volume 3E, https://t.ly/-gVK (accessed 01 September 2022).

31 Corruption Perception Index in Ghana, https://transparency.org/en/countries/ghana (accessed 01 September 2022).

32 Inside the world of Ghana's internet fraudsters, https://t.ly/G7GD (accessed 01 September 2022).

33 Ghana's Cybersecurity law implementation: CSOs demand more awareness creation, https://t.ly/Vma- (accessed 01 September 2022).

34 National Cyber Security Awareness Month, http://t.ly/M-RnW (accessed 01 September 2022).

prosecuting crimes lack content when it comes to the prosecution of offenders within the cyberspace. Furthermore, the lack of enforcement of legislation as well as the lack of resources for implementation by the technical units make it very difficult to combat cybercrime. Cybercrime will require technology and digital resources to be able to combat the threats of cybersecurity. Technical units tasked with the task of fighting cybercrime do not have the requisite infrastructure nor the motivation to put up a good fight against cybercrime.

II Ghana's Response to Cyberthreat

Despite Ghana's representation as a major cybercrime originating country, Ghana's effort has been remarkable when it comes to the fight against cybercrime. The 2020 Global Cybersecurity Index (GCI) report[35] of the International Telecommunications Union (ITU) ranked Ghana third (after Mauritius and Tanzania) as the best performing country in Africa in fighting cybercrime. This suggests that Ghana has developed a good regulatory framework to fight against cybercrime in the country.[36] Regulation is an important element in combatting cybercrimes as it goes into education, prevention, protection and enforcement. When a regulation is able to meet all these criteria, it could be deemed to promote lawfulness and also accelerate development[37] in a country. Ghana's regulatory framework towards the fight against cyber criminalities could be seen in the development of the Ghana National Cyber Security Policy and Strategy document[38] as well as the setting up of the National Cyber Security Centre (NCSC), under the Ministry of Communications.

The country has also made great legislative advancement all geared towards the protection of Ghanaians from the negative effects of internet use. There are a number of laws on the protection of persons in Ghana, particularly the protection of persons within the cyber ecosystem in Ghana. These are the Ghana Constitution 1992,[39] Criminal and other offences Act 1960 (ACT 29),[40] Evidence Act, 1975

35 Global Cybersecurity Index, 2020, https://t.ly/qpPc (accessed 01 September 2022).

36 In comparison to many African countries, Ghana's legal regime for combatting cybersecurity is quite robust. Despite the gains made recently in reviewing and enacting additional laws to combat cybercrime, the lack of enforcement and the resources for implementation leaves much to desire.

37 Haggard, MacIntyre and Tiede, The Rule of Law and Economic Development, Annu. Rev. Poli. Sci. 11:205–35, 2008, https://doi.org/10.1146/a nnurev.polisci.10.081205.100244 (accessed 01 September 2022).

38 Ghana National Cyber Security Policy and Strategy, Final Draft, 2014, https://t.ly/PkJd (accessed 01 September 2022).

39 The Ghana Constitution, 1992 (rev. 1996), https://constituteproject.org/constitution/Ghana_1996 (accessed 01 September 2022).

(N.R.C.D. 323),[41] The Foreign Exchange Act, 2006 (Act 723),[42] Anti-Money Laundering Act, 2008 (Act 749),[43] National Information Technology Agency Act, 2008 (Act 771),[44] Electronic Transactions Act 2008 (Act 772),[45] Electronic Communications Act 2008 (Act 775),[46] Economic and Organized Crime Office Act, 2010 (Act 804),[47] Mutual Legal Assistance Act, 2010 (Act 807),[48] Data Protection Act 2012 (Act 843),[49] Payment Systems and Services Act, 2019 (Act 987),[50] and the Cybersecurity Act 2020 (Act 1038).[51] A few of these laws are discussed briefly below.

III The Ghana Constitution 1992

The concept of data protection in Ghana finds its validation in the Constitution, specifically Article 18(2). This provision is to the effect that:

> No person shall be subjected to interference with the privacy of his home, property, correspondence or communication except in accordance with law and as may be necessary in a free and democratic society for public safety or the economic well-being of the country, for the protection of health or morals, for the prevention of disorder or crime or for the protection of the rights or freedoms of others.

This provision of the law is further expanded in some relevant statutes.

---

40 Criminal and other offences Act 29, 1960, https://t.ly/fXUl (accessed 01 September 2022).

41 Evidence Act, N.R.C.D. 323, 1975, https://lawsghana.com/pre_1992_legislation/NRC%20Decree/EVIDENCE%20ACT,%201975%20(NRCD%2 0323)/202 (accessed 01 September 2022).

42 The Foreign Exchange Act 723, 2006, p 168–186 https://t.ly/kbK2 (accessed 01 September 2022).

43 Anti-Money Laundering Act 749, 2008, p 2–28 https://t.ly/kbK2 (accessed 01 September 2022).

44 National Information Technology Agency Act 771, 2008, https://t.ly/EL_W (accessed 01 September 2022).

45 Electronic Transaction Act 772, 2008, https://t.ly/h2DV (accessed 01 September 2022).

46 Electronic Communications Act 775, 2008, https://nita.gov.gh/theevooc/2017/12/Electronic-Communications-Act-775.pdf (accessed 01 September 2022).

47 Economic and Organized Crime Office Act 804, 2010, https://t.ly/OULG (accessed 01 September 2022).

48 Mutual Legal Assistance Act 807, 2010, https://eoco.gov.gh/wp-content/uploads/2019/07/Mutual_Legal_Assistance_Act.pdf (accessed 01 September 2022).

49 Data Protection Act 843, 2012, https://nita.gov.gh/theevooc/2017/12/Data-Protection-Act-2012-Act-843.pdf (accessed 01 September 2022).

50 Payment Systems and Services Act. 987, 2019, https://www.bog.gov.gh/wp-content/uploads/2019/08/Payment-Systems-and-Services-Act -2019-Act-987-.pdf (accessed 01 September 2022).

51 Cybersecurity Act 1038, 2020, http://ir.parliament.gh/bitstream/handle/123456789/1800/CYBERSECURITY%20ACT%2C%202020%20%28A CT%201038%29.pdf?sequence=1 (accessed 01 September 2022).

IV The Electronic Transactions Act of 2008 (Act 772)

The Electronic Transactions Act of 2008 (Act 772) provides a framework for the usage of electronic transactions in court proceedings and the admissibility of evidence. It also regulates the incidences of transactions that are carried over the cyber ecosystem in Ghana. Some of the objectives of Act 772 are to provide for and facilitate electronic communications and related transactions in the public interest, to promote legal certainty and confidence in electronic communications and transactions, to develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions, to ensure that, in relation to the provision of electronic transactions services, the special needs of vulnerable groups and communities and persons with disabilities are duly taken into account[52] among others.

V Data Protection Act, 2012 (Act 843)

The importance of personal data protection also led to the enactment of the Data Protection Act, 2012 (Act 843) to protect personal data from violations and breaches by organizations, who are required to abide by a set of established principles and guidelines. Act 843 established the Data Protection Commission[53] with its core objective being the protection of the privacy of the individual and personal data. This is done through regulating the processing of personal data.[54] By ensuring that an individual's personal data is protected, Act 843 ensures that data collection must be done with prior consent of the data subject.[55] However, there are certain conditions under which the requirement to obtain prior consent can be waived. Some of these conditions are (i) when it necessary for the purpose of a contract to which the data subject is a party, (ii) authorized or required by law, (iii) to protect a legitimate interest of the data subject, (iv) necessary for the proper performance of a statutory duty, (v) or necessary to pursue the legitimate interest of the data controller or a third party to whom the data is supplied[56]. Under Act 843, the individual is accorded some rights. The Act ensures that data subjects have the right to consent, justification and objection to the processing of their personal data.[57] Data

52 Section 1 of Act 772.
53 Section 1 of Act 843.
54 Section 2 of Act 843.
55 Section 20 of Act 843.
56 Ibid.
57 Ibid.

subjects also have right to rectification, blocking, erasure and destruction of personal data.[58] A data subject has the right to prevent the processing of personal data for direct marketing.[59] It can, however, be argued that absolute right to privacy is not guaranteed since the exercise of such rights are subject to considerations of public ord, public safety, public morality, national security, or public interest[60], but the exclusion of these rights could lead to a state of arbitrariness. In further attempts to prevent arbitrariness, Act 843 puts a duty on a person who collects or processes personal data to observe the principles of accountability, lawfulness of processing, specification of purpose, compatibility of further processing with purpose of collection, quality of information, openness, data security safeguards, and data subject participation.[61]

VI Cybersecurity Act, 2020 (Act 1038)

Also, very significant and recent in the legislation on data protection, particularly, within the internet space is the Cybersecurity Act, 2020 (Act 1038). This Act establishes the Cyber Security Authority. Some of the functions of the Authority includes advising government and public institutions on matters relating to cybersecurity, certifying cybersecurity products and services, promoting the protection of children online, establishing and maintaining a framework for dissemination of information on cybersecurity, educating the public on cybercrime and cybersecurity, and collaborating with law enforcement agencies on matters relating to cybersecurity.[62] Act 1038 has been particularly celebrated as it prioritizes education and research,[63] criminalises some online offences such as child pornography,[64] and offers some protection as far as personal data is concerned when it comes to the application of a Subscriber Information.[65] It also created a specialized task force, the Computer Emergency Response Team (CERT-GH) both at the national level (NCERT) and at the sectorial level (SCERT).[66] Though considered as a good legislation, Act 1038 focuses on mainly regulatory structures and protocols with limited provision

58 Section 44 of Act 843.
59 Section 40 of Act 843.
60 Section 60 of Act 843.
61 Section 17 of Act 843.
62 Section 4 of Act 1038.
63 Section 69 & 70 of Act 1038.
64 Section 67 of Act 1038.
65 Ibid n (41).
66 Section 41–45 of Act 1038.

made on digital evidence, how to adduce digital forensics and how to overcome the difficulties in the subpoenaing of cybercriminals. Because of its rigid nature, the Act lacks adaptability to new forms of cybercrime. Act 1038 is also silent on specific acts like hacking, mobile money theft, data breaches, etc.

C Do these Laws Offer Protection to an Ordinary Ghanaian on the Internet?

Ghana has made significant effort in setting up specific institutions and enacting laws that are to promote the safety of the users of the internet. Though some of the laws have challenges, the laws, collectively in themselves, provide adequate level of protection of the privacy of the ordinary Ghanaian on the internet. Also, the provisions of the laws in Ghana largely fall within the regulatory framework of the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)[67]. The Malabo Convention sees Africa as a single entity on issues of data and privacy protection and suggests a harmonized legal and regulatory framework to protect all persons from processors and data controllers.

Although the current laws may be adequate, greater work has to do with the implementation of these laws that have been put in place and the enforcement of same. There is the need for adequate education on matters pertaining to the protection of personal data, the type of personal data of a person that should be put on the internet and basic safety protocols that should be observed when one uses the internet. That is, the roles individuals have to play for cyber predators to be caught up with the law and the preventive measures they can observe in order not to fall prey to internet predators.

Not so much effort is put into sensitization.[68] Sensitization, as and when it occurs, is done at certain level of education such as at universities but hardly will one find such exercises geared towards basic schools, markets communities and even to community centres in rural areas. Any effort to increase internet penetration should go hand in hand with sensitization on safety protocols. The month of October has been designated for cybersecurity awareness in Ghana. Hopefully, sensitization of the general public will be factored into activities to mark the celebrations of the cybersecurity month. Children must be educated on who (or who not) to interact with on the internet and a trusted adult must at all times supervise the use of internet by a child. This will help regulate some of the incidences related to

67 Ibid n (22).
68 Ibid n (33).

criminal activities related to children online. One of such activities being child pornography.

Another means of implementing the laws has to do with capacity building. The specialized taskforce must be trained to be effective and efficient in responding to issues that have to do with cybercrimes. Also, they must be well equipped with appropriate resources required to fight against predators in the Ghanaian cyber ecosystem. There must be legal reforms which should begin with intensive training for members of the judiciary on the roles they have to play in the fight against cyber criminals and ensuring that the privacy of every Ghanaian is protected on the internet. Developing and standardizing cyber security best practices is another means of implementing the laws and policies on cybersecurity in Ghana.

D Recommendation

Ghana must strengthen collaborations between authorities involved in data protection and cybersecurity. This includes law enforcement agencies and the judiciary to enhance seamless investigation into suspicious cyber activities, preservation of evidence relating to alleged cyber-criminal activities and the prosecution of cyber offenders. Law enforcement agencies ought to be properly coordinated to be able to fight organized crimes effectively and efficiently.

1. There must be harmonization of all policies and laws in the area of cybersecurity, data protection, digitization and digitalization.
2. In enacting new laws on cybersecurity and data protection, private sector involvement should be greatly encouraged.
3. Cybersecurity laws should not only be used as tools to fight crimes but should also be used to improve upon digitization and digitalization.
4. The Government should hold periodic reviews of the cybersecurity laws with the view of enhancing them to better address the dynamic cyber threats of the future. The government should partner with regional and international organizations like the Africa Union Development Agency-New Partnership for Africa's Development (AUDA-NEPAD), the European Union, the US Department of State and Department of Justice in identifying and working to close capacity gaps and meet international standards.
5. There is a lack of the culture of reporting cyber breaches among the populace of Ghana[69]. Most people are not even able to detect simple cyber threats when

69 Cyber Security in Ghana: Key Issues and Challenges Policy Brief (June, 2017), https://t.ly/rQeU (accessed 01 September 2022).

they do occur. The government should institute a sensitization programme that is designed to deliberately introduce cybersecurity into the cultures of the people.

6. Many of the high-level discussions on cybersecurity in the country have been delineated in workshops and conferences among stakeholders such as those in the tech industry and non-governmental organizations (NGOs). It is time to bring these same conversations of the law to the ordinary Ghanaian in the market centres, the streets, their shops and homes, community centres etc.
7. As the ICT sector is a rapidly evolving area, the government must continually acquire new and improved digital tools to protect law-abiding citizens to also apprehend cybercriminals.

E Conclusion

Ghana has several laws that cumulatively work to ensure some level of protection for the privacy of Ghanaians. There are some identified gaps regarding governance, regulation, enforcement and compliance of these laws. There is the need to build a resilient cyber ecosystem through regular, structured technical training, capacity building and engagement of the stakeholders. We must also review or improve on some of the existing legislation. e. g., The Criminal Act, 1960 (Act 29) and The Evidence Act, 1975 (N.R.C.D. 323) to bridge the gap of digitisation and digitalisation. The law enforcement agencies must be equipped with all the needed resources (human and material) to be able to keep up with the ever-changing ICT sector and the criminals who continually evolve new ways to take advantage of innocent users. The relevant ministry and agencies must continue their effort on public engagement and sensitization at all levels to educate the masses on the potential threats on the internet and how to avoid them. The national identification system (re-registration, verification of existing data, regular verification of registration instruments, passport, driver's license, voters ID) should be reliable and solid.

Finally, there are a number of laws relating to the protection of privacy in Ghana. A lot more has to be done to make them potent.

F Bibliography

Acheampong, The State of Information and Communication Technology and Health Informatics in Ghana, OJPHI 4(2):4191, 2012, pp 1–13.

African Union Convention on Cyber Security and Personal Data Protection, https://t.ly/qkkp. (accessed 01 September 2022).

Anti-Money Laundering Act 749, 2008, pp 2–28, https://t.ly/kbK2 (accessed 01 September 2022).

Baylon and Antwi-Boasiako, Increasing internet connectivity while combating cybercrime: Ghana as a case study, Centre for International Governance Innovation and Chatham House Paper Series: NO. 44, 2016, https://t.ly/3zlN (accessed 01 September 2022).

Convention on Cybercrime, https://rm.coe.int/1680081561 (accessed 01 August 2022).

Corruption Perception Index in Ghana, https://transparency.org/en/countries/ghana (accessed 01 September 2022).

Criminal and other offences Act 29, 1960, https://t.ly/fXUl (accessed 01 September 2022).

Cyber Security in Ghana: Key Issues and Challenges Policy Brief (June, 2017), https://t.ly/rQeU (accessed 01 September 2022).

Cybercrime victims lose an estimated $318 billion annually, https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/ (accessed 01 August 2022).

Cybersecurity Act 1038, 2020, http://ir.parliament.gh/bitstream/handle /123456789/1800/ CYBERSE CURITY%20ACT%2C%202020%20%28ACT%201038%29.pdf?sequence=1 (accessed 01 September 2022).

Data Protection Act 843, 2012, https://nita.gov.gh/theevooc/2017/12/Data-Protection-Act-2012-Act-843.pdf (accessed 01 September 2022).

Kemp, Digital 2022: Ghana, https://datareportal.com/reports/digital-2022-ghana (accessed 27 June 2022).

Digital Financial Services Policy, https://mofep.gov.gh/sites/default/files/acts/Ghana_DFS_Policy.pdf (accessed 01 August 2022).

Economic and Organized Crime Office Act 804, 2010, https://t.ly/OULG (accessed 01 September 2022).

ECOWAS Regional Critical Infrastructure Protection Policy, https://t.ly/NMMAj (accessed 01 September 2022).

Electronic Communications Act 775, 2008, https://nita.gov.gh/theevooc/2017/12/Electronic-Communications-Act-775.pdf (accessed 01 September 2022).

Electronic Transaction Act 772, 2008, https://t.ly/h2DV (accessed 01 September 2022).

Evidence Act, N.R.C.D. 323, 1975, https://lawsghana.com/pre_1992_legislation/NRC%20 Decree/EVIDENCE%20ACT,%201975%20(NRCD%20323)/202 (accessed 01 September 2022).

Ghana – Country Commercial Guide, https://www.trade.gov/country-commercial-guides/ghana-information-and-communications-technology-ict (accessed 27 June 2022).

Ghana 2021 Population and Housing Census, General Report Volume 3E, https://t.ly/-gVK (accessed 01 September 2022).

Ghana e-Government Interoperability Framework, https://nita.gov.gh/theevooc/2017/1 2/Ghana-eGovernment-Interoperability-Framework.pdf (accessed 01 August 2022).

Ghana loses $230 m to cyber criminals – CID, https://t.ly/7hlX (accessed 01 September 2022).

Ghana loses more than $114 m to cybercrime in two years, https://t.ly/ymFr (accessed 3 November 2022).

Ghana National Cyber Security Policy and Strategy, Final Draft, 2014, https://t.ly/PkJd. (accessed 01 September 2022).

Ghana Police Service Cyber Crime Unit, https://police.gov.gh/en/index.php/cyber-crime (assessed 01 September 2022).

Ghana Population Clock, https://t.ly/u9aXB (accessed 27 June 2022).

Ghana ranked third in Africa on Global Cybersecurity Index, https://t.ly/HKzWF (accessed 19 July 2022).

Ghana records over 11,000 cybercrime cases since 2019, https://www.graphic.com.gh/news/general-news/ghana-records-over-11-000-cybercrime-cases-in-a-year.html (accessed 01 September 2022).

Ghana's Cybersecurity law implementation: CSOs demand more awareness creation, https://t.ly/Vma- (accessed 01 September 2022).
Global Cybersecurity Index, 2020, https://t.ly/qpPc (accessed 01 September 2022).
Global internet penetration rate as of July 2022, by region, https://t.ly/MBuy (accessed 01 August 2022).
Haggard, MacIntyre and Tiede, The Rule of Law and Economic Development, Annu. Rev. Poli. Sci. 11:205–35, 2008 https://doi.org/10.1146/annurev.polisci.10.081205.100244 (accessed 01 September 2022).
Inside the world of Ghana's internet fraudsters, https://t.ly/G7GD (accessed 01 September 2022).
Mutual Legal Assistance Act 807, 2010, https://eoco.gov.gh/wp-content/uploads/2019/07/Mutual_Legal_Assistance_Act.pdf (accessed 01 September 2022).
National Broadband Policy and Implementation Strategy, 2012, https://nca.org.gh/wp-content/uploads/2020/09/National-Broadband-Policy-and-Implementation-Strategy.pdf (accessed 01 August 2022).
National Cyber Security Awareness Month, http://t.ly/M-RnW (accessed 01 September 2022).
National Information Technology Agency Act 771, 2008, https://t.ly/EL_W (accessed 01 September 2022).
National Science Technology and Innovation (STI) Policy, 2010, http://www.ecowrex.org/system/files/repository/2010_national-science-technology-and-innovation-policy_m.e.s.t.-ghana.pdf (accessed 01 August 2022).
National Telecommunications Policy, 2005, https://www.researchictafrica.net/countries/ghana/National_Telecommunications_Policy_ 20 05.pdf (accessed 01 August 2022).
Number of people living in extreme poverty in Ghana from 2016 to 2022, by area, https://t.ly/KBhR (accessed 01 September 2022).
Ouassini and Amini, Cybersecurity in Ghana, past, future and the present, in: Romaniuk and Manjikian (eds), Routledge Companion to Global Cyber-Security Strategy, pp 564–572.
Payment Systems and Services Act. 987, 2019, https://www.bog.gov.gh/wp-content/uploads/2019/08/Payment-Systems-and-Services-Act-2019-Act-987-.pdf (accessed 01 September 2022).
Percentage change in internet usage in West Africa between 2000 and 2021, by country, https://t.ly/CLK9 (accessed 01 August 2022).
Quarshie and Ami-Narh, The Growth and Usage of Internet in Ghana, JETCIS 3(9):1302–1308, 2012, pp 1302–1308.
Share of internet users in Africa as of January 2022, by country, https://t.ly/Fkgt (accessed 01 August 2022).
The Foreign Exchange Act 723, 2006, https://t.ly/kbK2. pp 168–186 (accessed 01 September 2022).
The Ghana Constitution, 1992, https://constituteproject.org/constitution/Ghana_1996 (accessed 01 September 2022).

Aishat O. Salami and Ridwan Oloyede

Digital Identity, Surveillance, and Data Protection in Africa

A Introduction

A digital identity is a collection of electronically captured and stored identity attributes[1] that uniquely describes a person within a given context and is used for electronic transactions. It provides remote assurance that the person is who they purport to be.[2] Digital identity serves as a way to prove your identity in a safe and secure way when accessing services or completing transactions online. It does this by removing the need to prove your identity through face-to-face interactions and by using physical identity documents.[3]

Digital transformation has become critical in today's world, necessitating increased use of digital identity. The increase in e-commerce and remote interactions, which have been accelerated by the Covid-19 pandemic, have also contribut-

1 Identity Attributes can be biographic data (*eg*, name, age, gender, address), biometric data (*eg*, fingerprints, iris scans, handprints).

2 Data Visualization, ID4D, https://id4d.worldbank.org/global-dataset/visualization (accessed 9 March 2023).

3 NSW Government, https://www.nsw.gov.au/nsw-government/projects-and-initiatives/future-digital-identity/digital-identity-is-important#:~:text=are%20the%20benefits%3F-,Digital%20identity%20and%20verifiable%20credentials%20provide%20a%20trusted%20and%20reliable,the%20digital%20world%20with%20confidence (accessed 13 September 2022).

https://doi.org/10.1515/9783110797909-009

ed to its increasing use. The importance of having a digital identity in a digitised economy cannot be overemphasised, as identity gaps create obstacles to participation in social, economic, and political life.[4] Notably, digital ID is increasingly becoming central to the effectiveness of technological innovations.[5] More and more individuals now require the use of digital ID systems to conduct day-to-day activities or access a number of services. In fact, in several instances, access to social and governmental benefits is dependent on having a valid digital identity.[6]

Furthermore, when making payments, applying for jobs, or exchanging health data, we frequently provide proof of identity. From e-passports to refugee registration cards, from online banking records to our social media profiles, digital ID programmes enable us to travel, do business, access services, and stay connected.[7] The reality now is such that presentation and verification of personal identity documents are required in many cases, such as to open a bank account in one's name, access healthcare, receive a pension payment, register for school, or file a court petition.[8]

Consequently, digital identity has been applauded for being pivotal in enabling increased social inclusion, financial inclusion, national security, the prevention of crime, the prevention of electronic fraud, election fraud, access to benefits, contributions to trade exchanges, e-commerce and transactions, and facilitating the movement of people across Africa.[9] For instance, digital ID makes it easier to track financial transactions, assists financial institutions in accurately verifying the identities of their customers[10] and prevents unauthorised access. In countries such as Thailand and Nigeria, the implementation of a digital ID system enabled

4 *Agence pour le Développement du Numérique*, A Look at Benin eID Experience, https://adn.bj/wp-content/uploads/2019/08/lookatbenin.pdf (accessed 14 September 2022).

5 Hall, "An Unparalleled Opportunity": Experts Discuss Digital ID's Potential to Unlock Fintech in Government, Global Government Fintech, https://www.globalgovernmentfintech.com/potential-for-digital-id-to-unlock-fintech-in-government-expert-discussion/ (accessed 19 November 2022).

6 Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable, World Bank, https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable (accessed 19 November 2022).

7 Adewole, Payment for Passport Application Now Digital, Says FG, Punch Newspaper, https://punchng.com/payment-for-passport-application-now-digital-says-fg/ (accessed 19 November 2022).

8 The State of Identification Systems in Africa, World Bank, http://documents1.worldbank.org/curated/en/298651503551191964/pdf/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf (accessed 10 November 2022).

9 African Union to Consider Good Digital Identity Principles at Summit, Omidyar Network, https://medium.com/omidyar-network/african-union-to-consider-good-digital-identity-principles-at-summit-c82ba87b1ae (accessed 20 November 2022).

10 Trulioo opens Global Gateway to Nigeria and Ghana, Finextra, https://www.finextra.com/pressarticle/80868/trulioo-opens-globalgateway-to-nigeria-and-ghana (accessed 19 November 2022).

the countries to expand their health insurance coverage[11] from 71% to 95% in less than two years and to remove about 60,000 ghost workers from the civil service, respectively.[12]

B State of Digital Identity

Globally, a few countries are committing to building national digital identity systems. This goal is further promoted by the World Bank's Identity for Development Initiative (ID4D)[13] and the United Nations Sustainable Development Goal (SDG 16.9).[14] The goal is to give everyone a legal identity, such as free birth registration, by 2030. Given the challenges involved in identifying citizens, especially in rural and less accessible areas, considerable efforts have been made and will continue to be made. Regardless, there are gaps in the rollout of identification systems. In this regard, it has been stated that,

> Although this goal may seem far away given the challenges that still stand in the efforts to democratize identity globally, most countries are making considerable prgress to ensure that their citizens have a legal identity[15].

In developing countries, where many people do not have legal names or other forms of identification, the identification gap is more obvious. The World Bank estimates that "one billion people around the world, most of them living in Africa and Asia, do not have documentation that proves their legal identities."[16] In contrast, many developed countries have digital identity management systems in place for things like education, national security, employment, financial services and welfare services.[17] The European Union, for instance, has adopted an

11 The Role of Digital Identification for Healthcare, the Emerging Use Cases, World Bank, https://documents1.worldbank.org/curated/en/595741519657604541/The-Role-of-Digital-Identification-for-Healthcare-The-Emerging-Use-Cases.pdf (accessed 19 November 2022).

12 Gelb and Clark, Identification for Development: The Biometrics Revolution, https://papers.ssrn.com/abstract=2226594 (accessed 9 March 2023).

13 Home, ID4D, https://id4d.worldbank.org/ (accessed 9 March 2023).

14 Goal 16, Department of Economic and Social Affairs, https://sdgs.un.org/goals/goal16 (accessed 9 March 2023).

15 What Is Digital Identity and Why Is It So Important?, Alice Biometrics, https://alicebiometrics.com/en/what-is-digital-identity-and-why-is-it-so-important/ (accessed 19 November 2022).

16 Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable, World Bank.

17 Gelb and Clark.

eIDAS[18] regulation for EU citizens and businesses to facilitate electronic identification, trust services and the exchange of administrative documents across the region.[19] The European Commission also reviewed the eIDAS framework with an open consultation (from 24 July to 2 October 2020) to collect feedback from key stakeholders of the eIDAS ecosystem and the general public.[20]

The lack of strong foundational identity systems is one of the main things that holds back Africa's identity system. Statistics from the UNICEF Annual Report 2014[21] reveal that "less than 45% of Sub-Saharan African children under the age of five have been registered, in contrast to 98% in Central and Eastern Europe, 92% in Latin America and the Caribbean, and over 75% in East Asia".[22] The birth registration rates are too low to provide a strong foundation for a national ID. This foundational identity issue has been linked to factors such as: the proliferation of disconnected identity registers. In Nigeria, for instance, there are "at least 13 federal agencies and different state agencies that offer digital identity services, and most are not interoperable.[23] In addition, the inability of users to access identity systems and services and the lack of infrastructure and resources to fund effective identity systems, add to the list of challenges.

Still, some of these basic ID problems can be fixed by making sure that identity management systems in African countries are harmonised. Harmonisation will allow for interoperability among the identity registries. In addition, the system should be reviewed to allow for easy access to digital identity systems and the integration of inclusive identity management systems.

Despite the concerns with digital identity on the continent, digital identity is seeing some remarkable developments among a number of African countries.[24] This is further encouraged by policy instruments such as the Digital Transforma-

18 Shaping Europe's Digital Future – eIDAS Regulation, European Commission, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (accessed 9 March 2023).

19 Lalancette, The importance of digital identity, FINN Partners, https://www.finnpartners.com/uk/news-insights/the-importance-of-digital-identity/ (accessed 9 March 2023).

20 Ibid (n. 20).

21 UNICEF Annual Report 2014, https://www.unicef.org/reports/unicef-annual-report-2014 (accessed 19 November 2022).

22 *Ibid.*

23 Strategic Roadmap for Digital Identity in Nigeria, NIMC, https://nimc.gov.ng/docs/reports/strategicRoadmapDigitalID_Nigeria_May2018.pdf (accessed 30 September 2022).

24 African Countries Embracing Biometrics, Digital IDs, Africa Renewal, https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids (accessed 19 November 2022).

tion Strategy (DTS) for Africa (2020–2030)[25], the digital-ID policy framework[26] and the expected benefit of DIs to the successful implementation of the African Continental Free Trade Area (AfCFTA)[27].

Tab. 1: Exemplary Overview of Digital Identity Frameworks

S/N	Country	Digital Identity Framework	Existence of Legal Authority	Existence of Data Protection Law	Existence of Data Protection Authority
1	Nigeria	National Identity Number (NIN)[28]	Present (The National Identity Management Commission)[29]	Nigeria Data Protection Act[30] The Nigerian Data Protection Regulation, 2019 ('NDPR')[31] however, provides legal safeguards for the processing of personal data in the country.	Present Nigeria Data Protection Commission.[32]
2	Ghana	Ghana Card	Present (The National Identification Authority)[33]	Present (Ghana Data Protection Act)[34]	Present (Ghana Data Protection Commission (DPC))[35]

25 Digital Transformation Strategy for Africa, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf (accessed 22 November 2022).
26 EVENT: Help the African Union Commission Develop a Digital ID Framework for the Continent, Africa Portal, https://www.africaportal.org/features/event-help-african-union-commission-develop-digital-id-framework-continent/ (accessed 9 March 2023).
27 Okunoye, Digital Identity in Nigeria, https://researchictafrica.net/wp/wp-content/uploads/2021/11/Nigeria_31.10.21.pdf (accessed 9 November 2022).
28 The NIN is an 11-digit number assigned to citizens upon data collection.
29 National Identity Management Commission, https://nimc.gov.ng/ (accessed 19 November 2022).
30 Nigeria Data Protection Act, https://ndpc.gov.ng/Files/Nigeria_Data_Protection_Act_2023.pdf (accessed 4 October 2023).
31 Nigeria Data Protection Regulation, https://ndpb.gov.ng/Files/NigeriaDataProtectionRegulation.pdf (accessed 15 September 2022).
32 'Home Page – NDPC' (Ndpc.gov.ng2023) <https://ndpc.gov.ng/> accessed 4 October 2023.
33 National Identification Authority, https://nia.gov.gh/ (accessed 19 November 2022).
34 The Data Protection Act 2012, Data Protection Commission Ghana, https://www.dataprotection.org.gh/data-protection/data-protection-acts-2012 (accessed 19 November 2022).
35 Data Protection Commission (DPC), Ghana.GOV, https://www.ghana.gov.gh/mdas/e1eca9de96/ (accessed 19 November 2022).

Tab. 1: Exemplary Overview of Digital Identity Frameworks *(Continued)*

S/N	Country	Digital Identity Framework	Existence of Legal Authority	Existence of Data Protection Law	Existence of Data Protection Authority
3	Republic of Benin		Present (Ministry of Interior and Public Security)	Generally governed by Law No. 2017–20 of April 20, 2018, on the digital code and Law No. 2009–09 of May 22, 2009, dealing with the Protection of Personally Identifiable Information	Present **(**The Beninese Data Protection Authority (APDP))[36]
4	Kenya	National Integrated Identification Management Systems (NIIMS) or Huduma Namba[37]	Present (Kenya Ministry of Interior)	Present (Kenya Data Protection Act)	Present (Office of the Data Protection Commissioner Kenya)
5	India	Aadhaar scheme[38][39]	Present (Unique Identification Authority of India (UIDAI	Digital Personal Data Protection Act[40]	Absent

36 Benin – Data Protection Authority (APDP) | APDP, https://apdp.bj/, (accessed 19 November 2022).
37 NIMS – NIIMS – National Integrated Identity Management System, nims, https://nims.co.ke/ (accessed 19 November 2022).
38 The Aadhar number is a unique, randomised 12- digit number given to residents.
39 Unique Identification Authority of India, Government of India, https://uidai.gov.in/ (accessed 19 November 2022).
40 Digital Data Protection Act https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf (accessed 4 October 2023).

C Problems Inherent in the Use of Digital Identity Systems

The extension of digital ID to every aspect of life creates a number of problems[41] for people. Digital identity is important, but if you look at digital identity systems as a whole, especially ones run by the government, you might be worried about how the information collected to prove people's identities is used and abused. In articulating the risk with the biometric identity system, the U.N. High Commissioner for Human Rights remarked that it is

> By definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is worrisome that some states are embarking on vast biometric data-based projects without having adequate legal and procedural safeguards in place.[42]

In the next few paragraphs, we will discuss some of the problems that can arise when digital identity systems are used.

First, digital ID registrations can be used to exclude and target people who are vulnerable. There is a fear that digital IDs will target and negatively impact the poorest and most marginalised individuals, who in most cases lack the means or are unable to access registration centres.[43] It can also be used to target and exclude people from some social and economic benefits.[44] "In 2017, about 22 percent of Gha-

---

41 Understanding Identity Systems Part 3: The Risks of ID, Privacy International, http://privacyinternational.org/explainer/2672/understanding-identity-systems-part-3-risks-id (accessed 9 March 2023).

42 Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, United Nations, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement (accessed 22 September 2022).

43 Africa RI and Van der Spuy, RIA Releases 10 Country Reports on Digital ID Framework, Research ICT Africa, https://researchictafrica.net/2021/11/09/ria-releases-10-country-reports-on-digital-id-framework/ (accessed 2 March 2023).

44 Exclusion by Design: How National ID Systems Make Social Protection Inaccessible to Vulnerable Populations, Privacy International, http://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible (accessed 9 March 2023).

naians identified a lack of ID as a reason for financial exclusion"[45]. Also, in 2021, it was reported[46] that up to a third of adults in Uganda, the majority of whom were women and elderly people, could not access social services and vital healthcare because they did not have the national ID card.[47]

Further, in situations where there are errors on the ID card, the vulnerable population easily suffers for it. For instance, 'correcting mistakes or replacing lost or stolen cards costs at least 50,000 Ugandan shillings (£10)' with a majority of Ugandans living on less than £1.30 daily[48]. So, people with low incomes are unable to get an ID card because it is too expensive to replace it or fix mistakes on it.

Furthermore, the lack of foundational identity systems in many African countries will result in vulnerable younger populations being unable to prove their identity and age due to a lack of the required breeder document, which is frequently the birth certificate.[49] This is true in many African countries, including Kenya and South Africa, where submitting breeder documents is a requirement for obtaining a digital ID.[50] The issue is highlighted during the Kenyan Huduma Namba rollout, where 'communities such as the Kenyan Nubian and Kenyan Somali communities, who have historically been discriminated against and denied citizenship, have no key documents such as birth certificates to show their nationality and are thus ineligible to be registered for a digital ID'.[51] With the rise in the number of governments making national identity mandatory before individuals can access some societal benefits,[52] there would be an increase in the number of people

45 Reimagining the Identity Ecosystems in SubSaharan Africa with Mobile, GSMA, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/12/Reimagining-identity-ecosystems-in-Sub-Saharan-Africa-with-mobile.pdf (accessed 27 November 2022).

46 Okiror, Uganda's ID Scheme Excludes Nearly a Third from Healthcare, Says Report, The Guardian, https://www.theguardian.com/global-development/2021/jun/09/ugandas-id-scheme-excludes-nearly-a-third-from-healthcare-says-report (accessed 20 November 2022).

47 *Ibid.*

48 Uganda Poverty Assessment 2016: Fact Sheet, World Bank, https://www.worldbank.org/en/country/uganda/brief/uganda-poverty-assessment-2016-fact-sheet (accessed 2 March 2023).

49 How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, Center for Human Rights and Global Justice https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf (accessed 16 November 2022).

50 Country Profiles Report, World Bank https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf accessed (16 September 2022).

51 Nubian Community in Kenya v. Kenya, https://www.justiceinitiative.org/litigation/nubian-community-kenya-v-kenya (accessed 19 November 2022).

52 Fighting Identity Systems, Privacy International, https://privacyinternational.org/impact/fighting-identity-systems (accessed 9 March 2023).

who, for varied reasons, are unable to obtain the national ID and would inevitably become excluded from such essential societal benefits to which they are entitled.[53]

The risk of exclusion can also be illustrated using persons with disabilities. For instance, where biometric data such as fingerprints or iris scans is a prerequisite to getting a digital identity, it would be impossible to capture a person born with adermatoglyphia,[54] or some other eye deformity. However, there are measures such as those in place in Tanzania, where other special identification marks such as a palm or toe print can be used instead of the disabled parts.[55]

Essentially, the exclusionary effect of being unable to register and get an ID card will, if upheld, be counter-productive to the goal of the identity system.[56] So, for a digital identity system to be inclusive, discriminatory practises must be stopped so that everyone has the same chance to use and benefit from the system.

As with different emerging technologies, when digital ID systems are used, there is also a risk to privacy and data security. As governments around the world collect and process data for their digital identity databases, the privacy and data protection rights of their citizens will inevitably be affected. This is exemplified by the decision of the Kenyan High Court in October 2021, which stopped the Huduma Namba project from going forward because there was not enough protection for the data of citizens.[57] The court ruled that "without specific provisions in place to protect citizens' data, the process of rolling out the cards would be illegal."[58] When the courts step in like this, it is a good thing because it will force governments to build and design their digital identity systems with the right safety features.

Cybersecurity risk is another problem that can arise when digital identity systems are used. There are a lot of threats to cyber security, which is another reason why cyber risks are a big worry for digital ID systems. A Foresight Africa 2022

---

53 Exclusion by Design: How National ID Systems Make Social Protection Inaccessible to Vulnerable Populations, Privacy International.

54 A genetic disorder of people born without fingerprints. Joseph Stromberg, 'Adermatoglyphia: The Genetic Disorder of People Born without Fingerprints' (Smithsonian Magazine14 January 2014) <https://www.smithsonianmag.com/science-nature/adermatoglyphia-genetic-disorder-people-born-without-fingerprints-180949338/> (accessed 15 September 2022).

55 Ensuring Socioeconomic Inclusion through Digital Identity, Global Voice Group, https://www.globalvoicegroup.com/news-article/ensuring-socioeconomic-inclusion-through-digital-identity/ (accessed 9 March 2023).

56 Digital Health: What Does It Mean for Your Rights and Freedoms, Privacy International, http://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms (accessed 9 March 2023).

57 Ensuring Socioeconomic Inclusion through Digital Identity, Global Voice Group.

58 *Ibid.*

study[59] reveals that cyberattacks cost African economies more than $3.5 billion even back in 2017. There is the cybersecurity incident that happened in July 2021, where a government database was hacked in Estonia,[60] with the hacker gaining access to the personal photos, names and other data attributes of over 280,000 Estonians. A number of African countries have also experienced a series of attacks. For instance, the Ugandan mobile money fraud hack.[61] The Nigerian National Information Management Commission (NIMC) has frequently had to publicly deny that there have been data breaches.[62]

In addition to the problems listed above, the push for identity systems has led to the growth of large biometric databases that can be used to track and profile people and groups. The identity database can be easily used to exploit, track and profile individuals since it links together diverse biometric and biographic attributes of an individual. This will easily enable governments to have an all-round view of personal and sensitive information about people. For instance, Nigeria's biometric database, among others, has been said to be a tool through which the government "monitors and silences dissidents and critics."[63]

---

59 Adeniran, Developing an Effective Data Governance Framework to Deliver African Digital Potentials, Brookings, https://www.brookings.edu/blog/africa-in-focus/2022/03/21/developing-an-effective-data-governance-framework-to-deliver-african-digital-potentials/ (accessed 20 November 2022).

60 Estonia Says a Hacker Downloaded 286,000 ID Photos from Government Database, The Record, https://therecord.media/estonia-says-a-hacker-downloaded-286000-id-photos-from-government-database/ (accessed 20 November 2022).

61 Uganda's Banks Have Been Plunged into Chaos by a Mobile Money Fraud Hack, Quartz, https://qz.com/africa/1915884/uganda-banks-mtn-airtel-hacked-by-mobile-money-fraudsters/ (accessed 20 November 2022).

62 Ukpe, NIMC Debunks Reports of Breach of Its Database, Nairametrics, https://nairametrics.com/2020/12/24/nimc-debunks-reports-of-breach-of-its-database/ (accessed 20 November 2022); Nwosa, Hacker: How I Breached NIMC Server, Stole over 3 million NINs' Data!, The New Diplomat, https://newdiplomatng.com/how-hacker-breached-nimc/ (accessed 20 November 2022); Our Servers Not Hacked, Remain Most Secure for Identity Management – NIMC, TVC News, https://www.tvcnews.tv/2022/01/our-servers-not-hacked-remain-most-secure-for-identity-management-nimc/ (accessed 20 November 2022).

63 "The Power to Surveil, Control, and Punish": The Dystopian Danger of a Mandatory Biometric Database in Mexico, Rest of World, https://restofworld.org/2021/the-dystopian-danger-of-a-mandatory-biometric-database-in-mexico/ (accessed 9 March 2023).

D African Union Digital ID Framework

The African Union Commission is "working towards the adoption of its policy framework on digital ID."[64] This is geared towards achieving Africa's Vision 2063[65] which aims to unify Africa and have transformed economies, and the Africa Union Digital Transformation Strategy (2020–2030)[66] which identifies inclusive and trusted digital ID systems as crucial. The purpose of the framework is to "define common requirements, governance mechanisms, and recommendations for further alignment between legal frameworks, while ensuring that all Africans can easily and securely access the services they require, when they require them, from both public and private sector providers."[67]

If fully implemented, the framework is expected to "contribute to the implementation of major continental initiatives such as the African Continental Free Trade Agreement, the Protocol on Free Movement of People, the African Passport and the Single African Air Transport Market."[68] It is also looked at as an instrument to further aid the interoperability and functioning of a more inclusive identity scheme in Africa.

E Emerging Trends and Issues in Africa's Digital Identity Landscape

Different African countries are increasingly implementing digital identity programmes.[69] In some cases, they are funded by foreign donor agencies and partners for a variety of purposes ranging from border control[70] to upgrading legacy and

64 EVENT: Help the African Union Commission Develop a Digital ID Framework for the Continent, Africa Portal.

65 Linking Agenda 2063 and the SDGs, African Union, https://au.int/agenda2063/sdgs (accessed 20 November 2022).

66 The Digital Transformation Strategy for Africa (2020–2030), African Union, https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030 (accessed 20 November 2022).

67 EVENT: Help the African Union Commission Develop a Digital ID Framework for the Continent, Africa Portal.

68 Partnership for Digital Identity Launched, Union Africaine, https://au.int/fr/node/35403 (accessed 20 November 2022).

69 African Countries Embracing Biometrics, Digital IDs, Africa Renewal.

70 Europe's Shady Funds to Border Forces in the Sahel, Privacy International, https://privacyinternational.org/news-analysis/3223/europes-shady-funds-border-forces-sahel (accessed 22 March 2023).

age-old national identity systems to encouraging the centralisation of identity systems. There is a shift toward modernising the age-old national identity system, as evidenced by the implementation and proposals to digitise civil registries. Countries like Rwanda,[71] Cameroon,[72] and Zimbabwe,[73] among other African countries, have taken measures to modernise their identity systems. There is also noticeable cooperation at the regional level on the biometric identity system. In West Africa, Nigeria announced plans to implement the ECOWAS biometric card in 2019.[74] WURI, a regional system that will enable the interoperability of digital identity systems, has been launched. This has been launched in countries like Togo[75] and Niger.[76]

Furthermore, sub-national units in some countries are adopting biometric based mandatory resident registration, thereby expanding the volume of government held data in different silos. For example, in Nigeria, states like Oyo[77] and Lagos[78] have resident registration systems. In July 2022, the Lagos state government launched the state's SMART ID card to enable more functionality, and it is biometric based.[79]

Additionally, there are an increasing number of private players in the digital identity ecosystem. This is evident in the rise of various digital identity companies

71 Rwanda Information Society Authority, Request for Consultation, https://www.risa.rw/index.php?eID=dumpFile&t=f&f=307&token=5539d9b29ead9b6488319c43a1e5a48560a75e13 (accessed 23 September 2022).

72 Civil Registration in Cameroon Is Being Modernised, https://www.giz.de/en/worldwide/87334.html (accessed 20 November 2022).

73 Digital Registry Services to Start by December, The Herald, https://www.herald.co.zw/digital-registry-services-to-start-by-december/ (accessed 20 November 2022).

74 Burt, Nigeria Moves to Implement Biometric ECOWAS Card with $41M MoU, Biometric Update, https://www.biometricupdate.com/201904/nigeria-moves-to-implement-biometric-ecowas-card-with-41m-mou (accessed 20 November 2022).

75 Hersey, Togo Signs MoU to Establish MOSIP Digital Identity System, Biometric Update, https://www.biometricupdate.com/202112/togo-signs-mou-to-establish-mosip-digital-identity-system (accessed 20 November 2022).

76 Burt, Niger Launches WURI Project to Issue Biometric ID for Regional Trade and Public Services, Biometric Update, https://www.biometricupdate.com/202210/niger-launches-wuri-project-to-issue-biometric-id-for-regional-trade-and-public-services (accessed 20 November 2022).

77 Insecurity: Oyo Begins Resident Registration Exercise with Transport Operators, Peoples Gazette, https://gazettengr.com/insecurity-oyo-begins-resident-registration-exercise-with-transport-operators/ (accessed 20 November 2022).

78 Bankole, LASRAA: Over 6.5M Residents Registered so Far, as Lagos Targets 10M by December – Sanwo-Olu, Vanguard, https://www.vanguardngr.com/2022/07/lasraa-over-6-5m-residents-registered-so-far-as-lagos-targets-10m-by-december-sanwo-olu/ (accessed 20 November 2022).

79 Lagos to Launch Smart ID Card for Residents, Tribune Online, https://tribuneonlineng.com/lagos-to-launch-smart-id-card-for-residents/ (accessed 20 November 2022).

in various African countries, offering various biometric and identity-based services ranging from identity authentication and authorisation, digital ID wallets, fraud prevention to inclusion promotion, among other value propositions.[80]

However, some of the trends are concerning. In some African countries, multiple government agencies collecting and enrolling in biometric-based identities is a recurring theme. In Nigeria, over ten different state and federal government agencies collect biometric identity systems and maintain their distinct systems[81] despite repeated directives for the agencies to harmonise their databases.[82]

Another trend identified in this research is mandatory SIM registration and mandatory SIM and national identity linkage requirements. According to a GSMA report in 2019, fifty African countries have mandatory SIM registration requirements,[83] and in a more recent report, there are only two countries without such a requirement.[84] Namibia, which is one of the countries without the requirement, has also launched a national initiative for mandatory SIM registration.[85] Mandatory SIM registration laws require telecommunications service providers to register subscribers' personal information and, in some cases, their biometrics before purchasing or activating a prepaid SIM card for their mobile device.[86] "Such laws can allow the state to identify the owner of a SIM card and infer who is likely to be making a call, sending a message, in a particular location at any particular

80 The Demand for Digital Verification Rises across Africa, Digital Banker Africa, https://digitalbankerafrica.com/the-demand-for-digital-verification-rises-across-africa/ (accessed 22 March 2023).
81 Assessing Data Protection, Tech Hive Advisory, https://techhiveadvisory.org.ng/wp-content/uploads/2022/06/Assessing-Data-Protection-1.pdf (accessed 16 November 2022).
82 Buhari Directs Agencies to Harmonise Collection, Usage of Biometric Data, Sundiata Post, https://sundiatapost.com/buhari-directs-agencies-to-harmonise-collection-usage-of-biometric-data/ (accessed 20 November 2022). Yusuf, Buhari Orders Biometric Collating Agencies to Harmonise Citizens Data before 2023, THISDAYLIVE, https://www.thisdaylive.com/index.php/2021/09/17/buhari-orders-biometric-collating-agencies-to-harmonise-citizens-data-before-2023/ (accessed 20 November 2022).
83 Access to Mobile Services and Proof of Identity, GSMA, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf (accessed 14 November 2022).
84 'Namibia Starts Mandatory SIM Registration Process – Connecting Africa' (Connecting Africa20 January 2023) <https://www.connectingafrica.com/author.asp?section_id=816&doc_id=782804> accessed 4 October 2023.
85 Nghiinomenwa-vali Erastus, 'Only two African countries with no SIM Card registration- CRAN, Eagle FM, https://www.eaglefm.com.na/news/only-two-african-countries-with-no-sim-card-registration-cran/ (accessed 20 November 2022).
86 Africa: SIM Card Registration Only Increases Monitoring and Exclusion, Privacy International, https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion, (accessed 20 November 2022).

time, or making a particular financial transaction."[87] Along with mandatory SIM registration, there is now a requirement to link SIM card registration to national identity registration systems.[88] Governments in Ghana,[89] Zambia,[90] Uganda,[91] and Nigeria[92] have made the announcement with threats and actual disconnection of subscribers' SIM cards that fail to meet the requirement after the expiration of the set deadlines.

The reasons typically cited for mandatory SIM registration range from national security, prevention and detection of crime and prevention of cybercrimes, among other reasons. However, there is scarce empirical evidence from these governments to demonstrate it systemically curbs or reduces crime.[93] However, criminals have found ways to increasingly outwit these systems. One of such ways is the emergence of a marketplace for pre-registered SIM cards,[94] that although illegal, remains a common practice.[95] In Nigeria, despite over a decade of mandatory SIM registration and two years of mandatory linkage between SIM registration and the national identity number, crime rates have not decreased systemically

87 *Ibid.*

88 Robert and Oloyede, Why Millions of Africans Are Right to Resist Mobile SIM Card Registration, Institute of Development Studies, https://www.ids.ac.uk/opinions/why-millions-of-africans-are-right-to-resist-mobile-sim-card-registration/ (accessed 20 November 2022).

89 Ghana to Block All Unregistered Sim Cards after October, Africa News https://www.africanews.com/2022/10/18/ghana-to-block-all-unregistered-sim-cards-after-october/> (accessed 20 November 2022).

90 Malakata, Zambia Has Deactivated Two Million SIM Cards so Far, ITWeb Africa, https://itweb.africa/content/Olx4z7kndVBv56km (accessed 20 November 2022).

91 Unlawful SIM Card Validation Exercise Is a Threat to Anonymity and Privacy, Unwanted Witness, https://www.unwantedwitness.org/unlawful-sim-card-validation-exercise-is-a-threat-to-anonymity-and-privacy/ (accessed 20 November 2022).

92 Azuh, NCC Orders Suspension of Numbers Registered without NIN and Stops SIM Card Sales, Tech Cabal, https://techcabal.com/2020/12/18/on-ncc-new-sim-card-regulation/ (accessed 20 November 2022).

93 Jentzsch, Implications of Mandatory Registration of Mobile Phone Users in Africa, Academia, https://www.academia.edu/23357252/Implications_of_mandatory_registration_of_mobile_phone_users_in_Africa?auto=download (accessed 20 November 2022).

94 Onaleye, FG Cracks down on Sale of Pre-Registered Sim Cards, Orders NCC to Block over 9 Million Sims, Technext, https://technext.ng/2019/09/13/fg-cracks-down-on-sale-of-pre-registered-sim-cards-orders-ncc-to-block-over-9-million-sims/ (accessed 20 November 2022).

95 "It Is a Criminal Offence to Buy Pre-Registered SIM Cards" - NCC Warns Telecom Consumers', NCC, https://www.ncc.gov.ng/stakeholder/media-public/news-headlines/588-it-is-a-criminal-offence-to-buy-pre-registered-sim-cards-ncc-warns-telecom-consumers (accessed 20 November 2022).

as a result of the registration.[96] In Ghana, despite the fact that the country's Minister of Communication and Digitalization recently stated that mandatory SIM card registration has reduced SIM card-related fraud, no data was presented.[97]

I Data Protection and Digital Identity

Privacy and data protection have been major concerns about the implementation of biometric and digital identity in Africa. There have been complaints about the lack of legal safeguards for the implementation of ID systems. A report published by CIPESA examining 23 African countries found that different African countries have adopted ID systems without appropriate safeguards to guarantee privacy and data protection for their citizens.[98] The countries fall short of the requirements under international human rights norms and principles 40 and 42 of the African Declaration on Freedom of Expression and Access to Information in Africa, which prescribe the right to privacy and data protection, the obligation of states to protect the right, and the need for a legal framework and an independent authority to enforce the law.[99]

At the time of this writing, thirty-six African countries have enacted data protection legislation.[100] Twenty-eight of these countries have established a new data protection authority, designated an existing one, or appointed members to it.[101]

---

96 Insecurity: Why Tracking Kidnappers Remains Difficult despite SIM-NIN Linkag, the Guardian Nigeria News - Nigeria and World News, https://guardian.ng/saturday-magazine/insecurity-why-tracking-kidnappers-remains-difficult-despite-sim-nin-linkage/ (accessed 20 November 2022).

97 Macdonald, Biometric SIM Registration Curbs Crime in Ghana, Not as Effective in Nigeria, Biometric Update, https://www.biometricupdate.com/202211/biometric-sim-registration-curbs-crime-in-ghana-not-as-effective-in-nigeria (accessed 20 November 2022).

98 Macdonald, Nearly Half of African Countries Lack Proper Safeguards for Biometric Data Collection, Biometric Update, https://www.biometricupdate.com/202211/nearly-half-of-african-countries-lack-proper-safeguards-for-biometric-data-collection (accessed 20 November 2022).

99 Declaration of Principles of Freedom of Expression and Access to Information in Africa, ACHPR, https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf (accessed 20 November 2022).

100 Tunisia, Morocco, Cabo Verde, Mauritania, Algeria, Mali, Niger, Senegal, Guinea, Cote d'Ivoire, Burkina Faso, Nigeria, Chad, Benin, Togo, Ghana, Gabon, Republic of Congo, Equatorial Guinea, Egypt, Angola, Zambia, Tanzania, Rwanda, Uganda, Kenya, Madagascar, Mauritius, Eswatini, South Africa, Somalia, Lesotho, the Seychelles, Botswana, Sao Tome and Principe, Democratic Republic of Congo, and Zimbabwe.

101 Benin, Angola, Algeria, Mauritania, Mauritius, Niger, Sao Tome and Principe, Nigeria, Senegal, Mali, Burkina Faso, Cote d'Ivoire, South Africa, Eswatini, Uganda, Kenya, Zimbabwe, Gabon, Rwanda, Ghana, Tunisia, Morocco, Botswana, Cape Verde, Tanzania, Somalia, Zambia, and Chad.

Ten of the countries with laws are yet to establish their authority,[102] and nineteen countries are yet to introduce data protection laws.[103] Additionally, there are legislative proposals in Namibia, South Sudan, Djibouti, The Gambia, Sierra Leone, Malawi, and Ethiopia.[104] According to the GSMA's 2021 report, some of the countries requiring mandatory SIM registration lack a data protection framework.[105]

Digital ID programmes are being introduced in countries without data protection laws. In Libya, a French company, Idemia, announced the signing of a Memorandum of Understanding "to develop a safe biometric identification system using facial recognition, fingerprints, and an iris scan for security and civil use".[106] Similarly, Guinea-Bissau has also adopted a biometric identity system. The absence of a data protection law and authority is a recurring theme between the two countries. The absence of law does not provide guarantees and safeguards for citizens to seek relief when there is abuse or misuse of their data.

In addition, there are countries that have data protection laws but have not yet designated a data protection authority to enforce them. Guinea launched an ID system without creating a data protection authority.[107] Lesotho is another example of a country implementing a digital ID system without the oversight of a data protection authority.[108] The problem with having a law without authority to enforce it is that it leaves individuals with inadequate data protection. In contrast, some countries began implementing their biometric identity systems without a data protection law, but later enacted or attempted to enact one. In Kenya, the digital identity programme, Huduma Namba, was invalidated by the court for violating the right

102 Seychelles, Guinea, Equatorial Guinea, Togo, Madagascar, Zambia, Tanzania, Lesotho, Egypt, and the Republic of Congo.

103 Namibia, South Sudan, Sudan, Libya, Guinea Bissau, Central Africa Republic, Cameroon, Somalia, Eritrea, Malawi, Mozambique, Burundi, the Democratic Republic of Congo, Comoros, Sierra Leone, Djibouti, Liberia, the Gambia, and Ethiopia, https://techhiveadvisory.africa/wp-content/uploads/2023/01/Round-up-of-data-protection-Africa-2022.pdf (accessed 22 March 2023).

104 'Infographics' (Privacy Lens) https://privacylens.africa/infographics/ (accessed 4 October 2023).

105 Digital Identity Access to Mobile Services and Proof of Identity, GSMA, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf (accessed 19 November 2022).

106 Libyan Interior Ministry Signs MoU with French Company Idemia for Biometric ID System, DailySabah, https://www.dailysabah.com/business/tech/libyan-interior-ministry-signs-mou-with-french-company-idemia-for-biometric-id-system (accessed 20 November 2022).

107 Burt, Guinea's Biometrics-Backed Foundational Identity Pilot Shows Open-Source Benefits, Biometric Update, https://www.biometricupdate.com/202011/guineas-biometrics-backed-foundational-identity-pilot-shows-open-source-benefits (accessed 20 November 2022).

108 Macdonald, Morocco, Lesotho Report Progress on Digital ID Ecosystems Development, Biometric Update, https://www.biometricupdate.com/202110/morocco-lesotho-report-progress-on-digital-id-ecosystems-development (accessed 20 November 2022).

to privacy under the Kenyan Constitution. Consequently, the government was directed to conduct a data protection impact assessment.[109] In Nigeria, the multiple biometric identity system started in the country long before the introduction of the data protection framework in 2019.[110] Similarly, the government of Madagascar received World Bank funding and launched the digital ID programme in 2020, before appointing members to the data protection commission two years later.[111] In addition, Togo announced the launch of its e-identity programme in 2021 as part of the government's 2025 digital transformation plan without establishing a data protection authority. [112]

Aside from the issues raised above, data protection authorities face a variety of challenges that limit their effectiveness. The problems include, among other things, a lack of independence, disregard by public institutions, a lack of political will, a lack of funding and human resources, outdated legislation, and the bundling of data protection with other mandates that overwhelm them.[113] Nevertheless, the lack of a strong data protection institution or legal framework leaves people vulnerable, and the risks associated with digital identity can be exacerbated in the absence of meaningful assistance.

II Surveillance: Creeping up with Citizens

One of the criticisms that has plagued the implementation of digital ID systems is the fear that the ID system will be used by the government for purposes other than legitimate ones.[114] The typical misuse cited is illegal and unjustified surveillance.[115]

---

109 Muthoni, Huduma Namba Declared Invalid, The Standard, https://www.standardmedia.co.ke/national/article/2001426183/huduma-namba-declared-invalid (accessed 20 November 2022).

110 Iruoma, ANALYSIS-Got Your Number: Privacy Concerns Hobble Nigeria's Digital ID Push, Reuters, https://www.reuters.com/article/nigeria-tech-rights-idUSL8N2OW2CJ (accessed 20 November 2022).

111 Macdonald, Madagascar Gets $143M World Bank Boost to Improve Its Digital ID Management System, Biometric Update, https://www.biometricupdate.com/202010/madagascar-gets-143m-world-bank-boost-to-improve-its-digital-id-management-system (accessed 20 November 2022).

112 Macdonald, Togo Hopes to Launch New Biometric ID Card in 2021, Biometric Update, https://www.biometricupdate.com/202012/togo-hopes-to-launch-new-biometric-id-card-in-2021 (accessed 20 November 2022).

113 Tech Hive Advisory '2021 Report Highlight, Tech Hive Advisory, https://techhiveadvisory.org.ng/wp-content/uploads/2021/08/Highlight-Report-min.pdf (accessed 27 November 2022).

114 Allen and Kelly, Deluge of Digital Repression Threatens African Security, Africa Center for Strategic Studies https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/ (accessed 22 March 2023).

Surveillance is inherently incompatible with the right to privacy. However, different governments have given varied reasons for conducting surveillance. Among the frequently cited reasons are national security, crime prevention and investigation, terrorism prevention, public safety, emergency preparedness, preserving a country's economic well-being, and putting international mutual agreements into effect.[116] The issue is exacerbated by the ID system because biometric data is collected by multiple government agencies and across sectors in some countries without adequate safeguards.[117] A recent study reported that 'African governments are spending over 1US$bn per year on digital surveillance technologies which are being used without adequate legal protections in ways that regularly violate citizens' fundamental human rights'[118]. In addition, ethnic profiling,[119]monitoring of dissidents, opponents, and rights activists, and access to biometric databases by law enforcement agents with minimal oversight and safeguards are some of the documented uses of government surveillance power.[120]

One of the concerns raised with mandatory SIM registration is the risk of government-led surveillance.[121] Governments continue to engage in secret mass surveillance without regard for adhering to human rights norms.[122] In Uganda, the

115 Babatunde Okunoye, 'Mistrust of Government within Authoritarian States Hindering User Acceptance and Adoption of Digital IDs in Africa: The Nigerian Context' (2022) 4 Data & Policy e37 https://www.cambridge.org/core/journals/data-and-policy/article/mistrust-of-government-within-authoritarian-states-hindering-user-acceptance-and-adoption-of-digital-ids-in-africa-the-nigerian-context/6511B7AE871C328F316912ACAD27274F, (accessed 4 October 2023).

116 Tony Roberts, Surveillance Laws in Africa, https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=y (accessed 22 March 2023).

117 *Ibid.*

118 'Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia', Institute of Development Studies, https://www.ids.ac.uk/publications/mapping-the-supply-of-surveillance-technologies-to-africa-case-studies-from-nigeria-ghana-morocco-malawi-and-zambia/ (accessed 4 October 2023).

119 Zelalem, Ethiopia Digital ID Prompts Fears of Ethnic Profiling, Context news, https://www.context.news/surveillance/ethiopia-digital-id-prompts-fears-of-ethnic-profiling (accessed 22 March 2023).

120 Bhalla, "Digital Authoritarianism" Threatening Basic Rights in Africa, Study Says, Reuters, https://www.reuters.com/article/us-rights-privacy-africa-trfn-idUSKBN2AW0YS (accessed 22 March 2023).

121 Africa: SIM Card Registration Only Increases Monitoring and Exclusion, Privacy International, http://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion (accessed 4 October 2023).

122 Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, United Nations, https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/SARAH%20MCKUNE.pdf (accessed 4 October 2023).

government used facial recognition enabled surveillance cameras to arrest protesters.[123] In Libya, the government signed a memorandum of agreement with a French digital ID company. According to the Interior Minister, it is to "develop a safe biometric identification system using facial recognition, fingerprints,and iris scans for security and civil use."[124] Some of the reasons cited include national security and the need to secure elections and prevent rigging.[125] In addition, the government said it asked Thales for "border surveillance using advanced technological systems to reduce crime and secure borders, which will enhance" the government's ability to monitor its people.[126] All these without a data protection law or an oversight authority. Similarly, foreign government funding is bolstering African governments' surveillance capabilities, most notably the EU funding of Niger's border control programme, which has been chastised for its lack of transparency.[127]

A report by the Institute of Development Studies demonstrated the increase in government funding for surveillance.[128] The study examined six African countries, and a noticeable pattern was the rise in government spending on surveillance tools in the absence of sufficient safeguards to protect human rights. In Togo, the infamous NSO group surveillance tool, Pegasus, has been documented by Citizenslab to be used on government critics, which included a priest.[129] The governments of Algeria, Botswana, Côte d'Ivoire, Egypt, Ghana, Malawi, Nigeria, Rwanda, South Africa, Tanzania, Uganda, Zambia, and Zimbabwe have been documented to have purchased and deployed surveillance tools.[130] To demonstrate the extent of abuse and

123 Kafeero, Uganda Is Using Huawei's Facial Recognition Tech to Crack down on Dissent after Anti-Government Protests, Quartz, https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters (accessed 20 November 2022).

124 Macdonald, Idemia to Help War-Torn Libya Establish Biometric Digital ID System, Biometric Update, https://www.biometricupdate.com/202011/idemia-to-help-war-torn-libya-establish-biometric-digital-id-system (accessed 22 March 2023).

125 *Ibid.*

126 *Ibid.*

127 'Europe's Shady Funds to Border Forces in the Sahel | Privacy International' http://privacyinternational.org/news-analysis/3223/europes-shady-funds-border-forces-sahel, (accessed 4 October 2023).

128 Ibid (117).

129 Scott-Railton, Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware – the Citizen Lab, The Citizen, https://citizenlab.ca/2020/08/nothing-sacred-nso-spyware-in-togo/ (accessed 20 November 2022).

130 Surveillance Technology a Concern for Many in Africa, NewAfricaDaily, https://newafricadaily.com/surveillance-technology-concern-many-africa (accessed 20 November 2022).

the lack of oversight, the governors of sub-national units in Nigeria have been accused of buying surveillance tools to monitor political opponents.[131]

Furthermore, law enforcement's access to personal data without safeguards raises concern. For example, in Nigeria, law enforcement can access subscriber databases without the oversight of the court, with the mere approval of the communication authority.[132] In February 2022, the Minister for Communications and the Digital Economy announced that the president had granted approval for law enforcement to have unfettered access to the databases of the National Identity Management Commission (NIMC) and the Nigerian Communication Commission (NCC).[133] A request for access to information made to the Minister requesting the implementation of safeguards went unanswered.[134] In this regard, there are lawsuits pending in court challenging the minister's decision to grant the law enforcement agencies access to ID databases.[135] While it is undeniable that there could be legitimate purposes for law enforcement to access these databases, the danger lies in the absence of judicial review, independent oversight mechanisms, repurposing of data, a notification mechanism, and the opportunity for appeal. The risk is amplified by documented instances of excesses displayed by law enforcement and the government. In addition, surveillance can be repurposed. In the 2022 United Nations report on privacy in the digital age, concerns were raised about the rise of state surveillance. The report noted,

> [w]hile purportedly being deployed for combating terrorism and crime, such spyware tools have often been used for illegitimate reasons, including to clamp down on critical or dissenting views and on those who express them, including journalists, opposition political figures and human rights defenders.[136]

---

131 Emmanuel, INVESTIGATION: How Governors Dickson, Okowa Spend Billions on High Tech Spying on Opponents, Others, Premium Times Nigeria, https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html (accessed 20 November 2022).

132 Article 8 Registration of Service Telephone Subscribers Regulations 2011.

133 Eleanya, Security Agencies Can Access NIN Database to Prevent, Solve Crimes – Pantami, Businessday, https://businessday.ng/interview/article/security-agencies-can-access-nin-database-to-prevent-solve-crimes-pantami/ (accessed 20 November 2022).

134 Press Statement, Ikigaination, https://ikigaination.org/press-statement/ (accessed 20 November 2022).

135 Ikigai Innovation Initiative Challenges the Federal Government and Its Agencies for Violations of Digital Rights, Ikigaination, https://ikigaination.org/ikigai-innovation-initiative-challenges-the-federal-government-and-its-agencies-for-violations-of-digital-rights/ (accessed 20 November 2022).

136 Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns, OHCHR, https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report (accessed 20 November 2022).

In addition, the report called for the restriction of the use of biometric recognition systems in public spaces.[137] According to the Acting U.N. High Commissioner for Human Rights, "digital technologies bring enormous benefits to societies. But pervasive surveillance comes at an excessive cost, undermining rights and choking the development of vibrant, pluralistic democracies."[138]

F Towards Best Practices

Different human rights instruments have defined key principles that should be present in a surveillance system. For the research, the principles serving as benchmark are derived from the Declaration on Freedom of Expression and Access to Information in Africa,[139] International Principles on the Application of Human Rights to Communications Surveillance,[140] and Draft UN Legal Instrument on Government-led Surveillance and Privacy.[141]

Tab. 2: Surveillance laws against international human rights metrics

Surveillance laws located in a single document
Define legitimate aim
Authorisation of independent competent judicial authority
Periodic review by independent oversight body
Legality – must be contained in a law
Existence of reasonable grounds
Necessary to secure evidence
Test if surveillance measure is proportionate and limited in scope
Notify individual subject of surveillance time to appeal and request due process
Annual transparency report published publicly on requests and autorisation

137 Ibid.
138 Ibid.
139 Principle 41, ACHPR.
140 Electronic Frontier Foundation, https://web.archive.org/web/20220423194002/ https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf (accessed 12 September 2022).
141 Draft Legal Instrument, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf (accessed 12 September 2022).

Conduct Human Rights Impact Assessment before deploying tools

Conduct surveillance for the most severe crimes

The metrics are derived from the principles set out in the following documents: the African Commission Declaration of Principles of Freedom of Expression and Access to Information in Africa[142], the International Principles on the Application of Human Rights to Communications Surveillance[143], and the UN Draft Instrument on Government-led Surveillance and Privacy[144].

The Institute of Development Studies report on the state of surveillance in Africa, which examined six African countries (Sudan, Egypt, Nigeria, Senegal, South Africa, and Kenya), discovered varying levels of adherence to these principles.[145] Of the six countries, South Africa had the most right-respecting legal framework.[146] Furthermore, in 2020, the Constitutional Court suspended the Regulation of Interception of Communications Act (RICA) for violation of the right to privacy by enabling mass surveillance.[147]

According to the report, various governments are passing laws to expand their legal surveillance powers, as well as conducting illegal surveillance on journalists, judges and members of the opposition parties. There have been laws introduced to weaken or break encryption. Most legal frameworks lack precision and privacy safeguards, and some laws lack a definition of legitimate aims. In addition, state agencies are found conducting surveillance beyond what is allowed by law, while at the same time, civil society is insufficient to hold the state fully accountable under the law, among other issues.[148]

142 'Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019' (African Commission on Human and Peoples' Rights, 17 April 2020) https://achpr.au.int/en/node/902 (accessed 4 October 2023).

143 Ibid (n. 144).

144 Ibid (n. 145).

145 Roberts, Mohamed Ali, Farahat, Oloyede and Mutung'u, Surveillance Law in Africa: a review of six countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.059.

146 Ibid (n. 119) 6.

147 Sonjica, Constitutional Court Declares Provisions of Rica Unconstitutional, TimesLIVE, https://www.timeslive.co.za/news/south-africa/2021-02-04-constitutional-court-declares-provisions-of-rica-unconstitutional/ (accessed 20 November 2022).

148 Ibid (n. 119)

G Recommendations

The importance, risks, and benefits of digital identity systems cannot be overstated as the world continues to digitise. The following recommendations are made for various stakeholders when integrating an inclusive, robust, trusted and responsible digital ID system:

I Governments

1. Enactment and implementation of data protection laws, with independent authorities to enforce the laws.
2. Take steps to improve the transparency and accountability of government procurement of surveillance technology.
3. Consideration for Data Protection Impact Assessment and Human Rights Impact Assessment before deploying ID systems or surveillance tools.
4. Formulation of inclusive policies that takes cognisance of gender disparities, and minority and marginalised groups.
5. Participation of all stakeholders and wider public consultations in the development of digital identity systems.
6. Need by Government to look beyond technological considerations, but also seek to remove the barriers to access and usage of digital ID.
7. Establishment of independent authorities with the authority to monitor data protection violations in the public and private sectors, conduct timely investigations of violations, receive complaints from individuals and organisations, and impose effective penalties for violations of the law.
8. Provision of legal identification free from discrimination to all relevant persons in a country.
9. Introduction of trust framework in identity management system.
10. Enhance mechanisms for the independent authorisation and oversight of State surveillance and ensure that these mechanisms have the necessary expertise and resources to monitor and enforce the legality, necessity and proportionality of surveillance measures.
11. Examine the laws to confirm that they do not mandate the blanket, indiscriminate surveillance, weaken encryption or excessively allow surveillance.

II Businesses

12. Respect the right to privacy and all other human rights consistent with their duty to do so. At the very least, businesses should fully implement the Guiding Principles on Business and Human Rights, which entails conducting effective human rights due diligence across their operations and in relation to all human rights, including the right to privacy, and taking appropriate action to prevent, mitigate and address actual and potential impacts.
13. Seek to ensure an elevated level of security and confidentiality for all communications and personal data transmitted, collected, stored, or otherwise handled. Conduct ongoing evaluations to determine how to best design and update the security of products and services.

H Conclusion

The immense benefit that digital ID offers is undeniable. However, it is an innovation that needs to be embraced with caution. Digital ID can amplify existing societal injustices like exclusion and discrimination. Additionally, privacy and security are growing concerns that must be addressed. The study highlighted the diverse legal and institutional landscape, the disregard for the legal framework, and the lack of surveillance safeguards. Even where it exists, the law is insufficient because the government is capable of disregarding its provisions.

To maximise the benefits of ID systems, there is a need to implement an approach that will advance fairness, justice, and human rights while preventing government and private intrusion. Laws and institutions must include safeguards against unchecked surveillance and abuse by law enforcement agencies. The emergence of private companies in the digital ID ecosystem highlights the need for stricter accountability and digital responsibility to prevent the commodification, abuse, misuse, and unlawful use and disclosure of personal data. Before being deployed, technical solutions must be tested against human rights impact assessments, and civil society must play a larger role than ever in holding government and private institutions accountable through advocacy, evidence-based research and strategic litigation. Overall, creating digital identities with human rights, privacy and data protection principles, inclusivity, and sustainability in mind will result in a transformative identity management system for the continent.

I Bibliography

"The Power to Surveil, Control, and Punish": The Dystopian Danger of a Mandatory Biometric Database in Mexico, Rest of World, https://restofworld.org/2021/the-dystopian-danger-of-a-mandatory-biometric-database-in-mexico/ (accessed 9 March 2023).

_Africa: SIM Card Registration Only Increases Monitoring and Exclusion, Privacy International, https://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion, (accessed 20 November 2022).

_African Countries Embracing Biometrics, Digital IDs, Africa Renewal, https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids (accessed 19 November 2022).

Allen and Kelly, Deluge of Digital Repression Threatens African Security, Africa Center for Strategic Studies https://africacenter.org/spotlight/deluge-digital-repression-threatens-african-security/ (accessed 22 March 2023).

Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General, United Nations, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement (accessed 22 September 2022).

Benin – Data Protection Authority (APDP) | NADPA-RAPDP, https://www.rapdp.org/en/node/38, (accessed 19 November 2022).

Bhalla, "Digital Authoritarianism" Threatening Basic Rights in Africa, Study Says, Reuters, https://www.reuters.com/article/us-rights-privacy-africa-trfn-idUSKBN2AW0YS (accessed 22 March 2023).

Buhari Directs Agencies to Harmonise Collection, Usage of Biometric Data, Sundiata Post, https://sundiatapost.com/buhari-directs-agencies-to-harmonise-collection-usage-of-biometric-data/ (accessed 20 November 2022).

Civil Registration in Cameroon Is Being Modernised, https://www.giz.de/en/worldwide/87334.html (accessed 20 November 2022).

Data Visualization, ID4D, https://id4d.worldbank.org/global-dataset/visualization (accessed 9 March 2023).

Declaration of Principles of Freedom of Expression and Access to Information in Africa, ACHPR, https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf (accessed ###).

Digital Health: What Does It Mean for Your Rights and Freedoms, Privacy International, http://privacyinternational.org/long-read/4671/digital-health-what-does-it-mean-your-rights-and-freedoms (accessed 9 March 2023).

Digital Transformation Strategy for Africa, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf (accessed 22 November 2022).

Draft Legal Instrument, https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf (accessed 12 September 2022).

Shaping Europe's Digital Future – eIDAS Regulation, European Commission, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (accessed 9 March 2023).

Electronic Frontier Foundation, https://web.archive.org/web/20220423194002/https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf (accessed 12 September 2022).

Ensuring Socioeconomic Inclusion through Digital Identity, Global Voice Group, https://www.globalvoicegroup.com/news-article/ensuring-socioeconomic-inclusion-through-digital-identity/ (accessed 9 March 2023).

Estonia Says a Hacker Downloaded 286,000 ID Photos from Government Database, The Record, https://therecord.media/estonia-says-a-hacker-downloaded-286000-id-photos-from-government-database/ (accessed 20 November 2022).

Europe's Shady Funds to Border Forces in the Sahel, Privacy International, https://privacyinternational.org/news-analysis/3223/europes-shady-funds-border-forces-sahel (accessed 22 March 2023).

EVENT: Help the African Union Commission Develop a Digital ID Framework for the Continent, Africa Portal, https://www.africaportal.org/features/event-help-african-union-commission-develop-digital-id-framework-continent/ (accessed 9 March 2023).

Exclusion by Design: How National ID Systems Make Social Protection Inaccessible to Vulnerable Populations, Privacy International, http://privacyinternational.org/long-read/4472/exclusion-design-how-national-id-systems-make-social-protection-inaccessible (accessed 9 March 2023).

Onaleye, FG Cracks down on Sale of Pre-Registered Sim Cards, Orders NCC to Block over 9 Million Sims, Technext, https://technext.ng/2019/09/13/fg-cracks-down-on-sale-of-pre-registered-sim-cards-orders-ncc-to-block-over-9-million-sims/ (accessed 20 November 2022).

Fighting Identity Systems, Privacy International, https://privacyinternational.org/impact/fighting-identity-systems (accessed 9 March 2023).

Data Protection Commission (DPC), Ghana.GOV, https://www.ghana.gov.gh/mdas/e1eca9de96/ (accessed 19 November 2022).

Goal 16, Department of Economic and Social Affairs, https://sdgs.un.org/goals/goal16 (accessed 9 March 2023).

Home, ID4D, https://id4d.worldbank.org/ (accessed 9 March 2023).

Home, National Information Technology Development Agency, NITDA, https://nitda.gov.ng/ (accessed 15 November 2022).

Ikigai Innovation Initiative Challenges the Federal Government and Its Agencies for Violations of Digital Rights, Ikigaination, https://ikigaination.org/ikigai-innovation-initiative-challenges-the-federal-government-and-its-agencies-for-violations-of-digital-rights/ (accessed 20 November 2022).

Insecurity: Why Tracking Kidnappers Remains Difficult despite SIM-NIN Linkag, the Guardian Nigeria News – Nigeria and World News, https://guardian.ng/saturday-magazine/insecurity-why-tracking-kidnappers-remains-difficult-despite-sim-nin-linkage/ (accessed 20 November 2022).

Linking Agenda 2063 and the SDGs, African Union, https://au.int/agenda2063/sdgs (accessed 20 November 2022).

National Identification Authority, https://nia.gov.gh/ (accessed 19 November 2022).

National Identity Management Commission, https://nimc.gov.ng/ (accessed 19 November 2022).

Nigeria Data Protection Regulation, https://ndpb.gov.ng/Files/NigeriaDataProtectionRegulation.pdf (accessed 15 September 2022).

NIMS – NIIMS – National Integrated Identity Management System, nims, https://nims.co.ke/ (accessed 19 November 2022).

Nubian Community in Kenya v. Kenya, https://www.justiceinitiative.org/litigation/nubian-community-kenya-v-kenya (accessed 19 November 2022).

Partnership for Digital Identity Launched, Union Africaine, https://au.int/fr/node/35403 (accessed 20 November 2022).

Press Statement, Ikigaination, https://ikigaination.org/press-statement/ (accessed 20 November 2022). https://paradigmhq.org/press-statementpin-ikigai/

Adewole, Payment for Passport Application Now Digital, Says FG, Punch Newspaper, https://punchng.com/payment-for-passport-application-now-digital-says-fg/ (accessed 19 November 2022).

Rwanda Information Society Authority, Request for Consultation, https://www.risa.rw/index.php?eID=dumpFile&t=f&f=307&token=5539d9b29ead9b6488319c43a1e5a48560a75e13 (accessed 23 September 2022).

SERAP to Sue Buhari for Granting Security Agencies Access to Data, https://punchng.com/nin-sim-linkage-serap-to-sue-buhari-for-granting-security-agencies-access-to-data/ (accessed 29 November 2022).

Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns, OHCHR, https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report (accessed 20 November 2022).

Strategic Roadmap for Digital Identity in Nigeria, NIMC, https://nimc.gov.ng/docs/reports/strategicRoadmapDigitalID_Nigeria_May2018.pdf (accessed 30 September 2022).

Surveillance Technology a Concern for Many in Africa, NewAfricaDaily, https://newafricadaily.com/surveillance-technology-concern-many-africa (accessed 20 November 2022).

The Data Protection Act 2012, Data Protection Commission Ghana, https://www.dataprotection.org.gh/data-protection/data-protection-acts-2012 (accessed 19 November 2022).

The Digital Transformation Strategy for Africa (2020–2030), African Union, https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030 (accessed 20 November 2022).

Lalancette, the importance of digital identity, FINN Partners, https://www.finnpartners.com/uk/news-insights/the-importance-of-digital-identity/ (accessed 9 March 2023).

Uganda Poverty Assessment 2016: Fact Sheet, World Bank, https://www.worldbank.org/en/country/uganda/brief/uganda-poverty-assessment-2016-fact-sheet (accessed 2 March 2023).

Uganda's Banks Have Been Plunged into Chaos by a Mobile Money Fraud Hack, Quartz, https://qz.com/africa/1915884/uganda-banks-mtn-airtel-hacked-by-mobile-money-fraudsters/ (accessed 20 November 2022).

Understanding Identity Systems Part 3: The Risks of ID, Privacy International, http://privacyinternational.org/explainer/2672/understanding-identity-systems-part-3-risks-id (accessed 9 March 2023).

UNICEF Annual Report 2014, https://www.unicef.org/reports/unicef-annual-report-2014 (accessed 19 November 2022).

Unique Identification Authority of India, Government of India, https://uidai.gov.in/ (accessed 19 November 2022).

What Is Digital Identity and Why Is It So Important?, Alice Biometrics, https://alicebiometrics.com/en/what-is-digital-identity-and-why-is-it-so-important/ (accessed 19 November 2022).

Adeniran, Developing an Effective Data Governance Framework to Deliver African Digital Potentials, Brookings, https://www.brookings.edu/blog/africa-in-focus/2022/03/21/developing-an-effective-data-governance-framework-to-deliver-african-digital-potentials/ (accessed 20 November 2022).

Africa RI and Van der Spuy, RIA Releases 10 Country Reports on Digital ID Framework, Research ICT Africa, https://researchictafrica.net/2021/11/09/ria-releases-10-country-reports-on-digital-id-framework/ (accessed 2 March 2023).

Ghana to Block All Unregistered Sim Cards after October, Africa News https://www.africanews.com/2022/10/18/ghana-to-block-all-unregistered-sim-cards-after-october/> (accessed 20 November 2022).

Agence pour le Développement du Numérique, A Look at Benin eID Experience, https://adn.bj/wp-content/uploads/2019/08/lookatbenin.pdf (accessed 14 September 2022).
Macdonald, Biometric SIM Registration Curbs Crime in Ghana, Not as Effective in Nigeria, Biometric Update, https://www.biometricupdate.com/202211/biometric-sim-registration-curbs-crime-in-ghana-not-as-effective-in-nigeria (accessed 20 November 2022).
Macdonald, Idemia to Help War-Torn Libya Establish Biometric Digital ID System, Biometric Update, https://www.biometricupdate.com/202011/idemia-to-help-war-torn-libya-establish-biometric-digital-id-system (accessed 22 March 2023).
Macdonald, Madagascar Gets $143M World Bank Boost to Improve Its Digital ID Management System, Biometric Update, https://www.biometricupdate.com/202010/madagascar-gets-143m-world-bank-boost-to-improve-its-digital-id-management-system (accessed 20 November 2022).
Macdonald, Morocco, Lesotho Report Progress on Digital ID Ecosystems Development, Biometric Update, https://www.biometricupdate.com/202110/morocco-lesotho-report-progress-on-digital-id-ecosystems-development (accessed 20 November 2022).
Macdonald, Nearly Half of African Countries Lack Proper Safeguards for Biometric Data Collection, Biometric Update, https://www.biometricupdate.com/202211/nearly-half-of-african-countries-lack-proper-safeguards-for-biometric-data-collection (accessed 20 November 2022).
Macdonald, Togo Hopes to Launch New Biometric ID Card in 2021, Biometric Update, https://www.biometricupdate.com/202012/togo-hopes-to-launch-new-biometric-id-card-in-2021 (accessed 20 November 2022).
Yusuf, Buhari Orders Biometric Collating Agencies to Harmonise Citizens Data before 2023, THISDAYLIVE, https://www.thisdaylive.com/index.php/2021/09/17/buhari-orders-biometric-collating-agencies-to-harmonise-citizens-data-before-2023/ (accessed 20 November 2022).
Okunoye, Digital Identity in Nigeria, https://researchictafrica.net/wp/wp-content/uploads/2021/11/Nigeria_31.10.21.pdf (accessed 9 November 2022).
Azuh, NCC Orders Suspension of Numbers Registered without NIN and Stops SIM Card Sales, Tech Cabal, https://techcabal.com/2020/12/18/on-ncc-new-sim-card-regulation/ (accessed 20 November 2022).
How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons, Center for Human Rights and Global Justice https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf (accessed 16 November 2022).
Burt, Guinea's Biometrics-Backed Foundational Identity Pilot Shows Open-Source Benefits, Biometric Update, https://www.biometricupdate.com/202011/guineas-biometrics-backed-foundational-identity-pilot-shows-open-source-benefits (accessed 20 November 2022).
Burt, Niger Launches WURI Project to Issue Biometric ID for Regional Trade and Public Services, Biometric Update, https://www.biometricupdate.com/202210/niger-launches-wuri-project-to-issue-biometric-id-for-regional-trade-and-public-services (accessed 20 November 2022).
Burt, Nigeria Moves to Implement Biometric ECOWAS Card with $41M MoU, Biometric Update, https://www.biometricupdate.com/201904/nigeria-moves-to-implement-biometric-ecowas-card-with-41m-mou (accessed 20 November 2022).
Libyan Interior Ministry Signs MoU with French Company Idemia for Biometric ID System, DailySabah, https://www.dailysabah.com/business/tech/libyan-interior-ministry-signs-mou-with-french-company-idemia-for-biometric-id-system (accessed 20 November 2022).
Trulioo opens Global Gateway to Nigeria and Ghana, Finextra, https://www.finextra.com/pressarticle/80868/trulioo-opens-globalgateway-to-nigeria-and-ghana (accessed 19 November 2022).

Eleanya, Security Agencies Can Access NIN Database to Prevent, Solve Crimes – Pantami, Businessday, https://businessday.ng/interview/article/security-agencies-can-access-nin-database-to-prevent-solve-crimes-pantami/ (accessed 20 November 2022).

Hersey, Togo Signs MoU to Establish MOSIP Digital Identity System, Biometric Update, https://www.biometricupdate.com/202112/togo-signs-mou-to-establish-mosip-digital-identity-system (accessed 20 November 2022).

Gelb and Clark, Identification for Development: The Biometrics Revolution, https://papers.ssrn.com/abstract=2226594 (accessed 9 March 2023).4d

Reimagining the Identity Ecosystems in SubSaharan Africa with Mobile, GSMA, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/12/Reimagining-identity-ecosystems-in-Sub-Saharan-Africa-with-mobile.pdf (accessed 27 November 2022).

Access to Mobile Services and Proof of Identity, GSMA, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/ProofofIdentity2019_WebSpreads.pdf (accessed 14 November 2022).

Digital Identity Acess to Mobile Services and Proof of Identity, GSMA, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf (accessed 19 November 2022).

Hall, "An Unparalleled Opportunity": Experts Discuss Digital ID's Potential to Unlock Fintech in Government, Global Government Fintech, https://www.globalgovernmentfintech.com/potential-for-digital-id-to-unlock-fintech-in-government-expert-discussion/ (accessed 19 November 2022).

Nwosa, Hacker: How I Breached NIMC Server, Stole over 3 million NINs' Data!, The New Diplomat, https://newdiplomatng.com/how-hacker-breached-nimc/ (accessed 20 November 2022)

Bankole, LASRAA: Over 6.5M Residents Registered so Far, as Lagos Targets 10M by December – Sanwo-Olu, Vanguard, https://www.vanguardngr.com/2022/07/lasraa-over-6-5m-residents-registered-so-far-as-lagos-targets-10m-by-december-sanwo-olu/ (accessed 20 November 2022).

Scott-Railton, Nothing Sacred: Religious and Secular Voices for Reform in Togo Targeted with NSO Spyware – the Citizen Lab, The Citizen, https://citizenlab.ca/2020/08/nothing-sacred-nso-spyware-in-togo/ (accessed 20 November 2022).

Muthoni, Huduma Namba Declared Invalid, The Standard, https://www.standardmedia.co.ke/national/article/2001426183/huduma-namba-declared-invalid (accessed 20 November 2022).

Iruoma, ANALYSIS-Got Your Number: Privacy Concerns Hobble Nigeria's Digital ID Push, Reuters, https://www.reuters.com/article/nigeria-tech-rights-idUSL8N2OW2CJ (accessed 20 November 2022).

Malakata, Zambia Has Deactivated Two Million SIM Cards so Far, ITWeb Africa, https://itweb.africa/content/Olx4z7kndVBv56km (accessed 20 November 2022).

Insecurity: Oyo Begins Resident Registration Exercise with Transport Operators, Peoples Gazette, https://gazettengr.com/insecurity-oyo-begins-resident-registration-exercise-with-transport-operators/ (accessed 20 November 2022).

Nghiinomenwa-vali Erastus, 'ONLY TWO AFRICAN COUNTRIES with NO SIM CARD REGISTRATION-CRAN, Eagle FM, https://www.eaglefm.com.na/news/only-two-african-countries-with-no-sim-card-registration-cran/ (accessed 20 November 2022).

Jentzsch, Implications of Mandatory Registration of Mobile Phone Users in Africa, Academia, https://www.academia.edu/23357252/Implications_of_mandatory_registration_of_mobile_phone_users_in_Africa?auto=download (accessed 20 November 2022).

"It Is a Criminal Offence to Buy Pre-Registered SIM Cards" – NCC Warns Telecom Consumers', NCC, https://www.ncc.gov.ng/stakeholder/media-public/news-headlines/588-it-is-a-criminal-offence-to-buy-pre-registered-sim-cards-ncc-warns-telecom-consumers (accessed 20 November 2022).

Sonjica, Constitutional Court Declares Provisions of Rica Unconstitutional, TimesLIVE, https://www.timeslive.co.za/news/south-africa/2021-02-04-constitutional-court-declares-provisions-of-rica-unconstitutional/ (accessed 20 November 2022).

NSW Government, https://www.nsw.gov.au/nsw-government/projects-and-initiatives/future-digital-identity/digital-identity-is-important#:~:text=are%20the%20benefits%3F-,Digital%20identity%20and%20verifiable%20credentials%20provide%20a%20trusted%20and%20reliable,the%20digital%20world%20with%20confidence (accessed 13 September 2022).

Emmanuel, INVESTIGATION: How Governors Dickson, Okowa Spend Billions on High Tech Spying on Opponents, Others, Premium Times Nigeria, https://www.premiumtimesng.com/investigationspecial-reports/204987-investigation-governors-dickson-okowa-spend-billions-high-tech-spying-opponents-others.html (accessed 20 November 2022).

Okiror, Uganda's ID Scheme Excludes Nearly a Third from Healthcare, Says Report, The Guardian, https://www.theguardian.com/global-development/2021/jun/09/ugandas-id-scheme-excludes-nearly-a-third-from-healthcare-says-report (accessed 20 November 2022).

African Union to Consider Good Digital Identity Principles at Summit, Omidyar Network, https://medium.com/omidyar-network/african-union-to-consider-good-digital-identity-principles-at-summit-c82ba87b1ae (accessed 20 November 2022).

Roberts, Mohamed Ali, Farahat, Oloyede and Mutung'u, Surveillance Law in Africa: a review of six countries, Brighton: Institute of Development Studies, DOI: 10.19088/IDS.2021.059.

Kafeero, Uganda Is Using Huawei's Facial Recognition Tech to Crack down on Dissent after Anti-Government Protests, Quartz, https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters (accessed 20 November 2022).

Stromberg, Adermatoglyphia, Smithsonian Magazine, https://www.smithsonianmag.com/science-nature/adermatoglyphia-genetic-disorder-people-born-without-fingerprints -180949338/ (accessed 15 September 2022).

Tech Hive Advisory '2021 Report Highlight, Tech Hive Advisory, https://techhiveadvisory.org.ng/wp-content/uploads/2021/08/Highlight-Report-min.pdf (accessed 27 November 2022).

Assessing Data Protection, Tech Hive Advisory, https://techhiveadvisory.org.ng/wp-content/uploads/2022/06/Assessing-Data-Protection-1.pdf (accessed 16 November 2022).

Digital Registry Services to Start by December, The Herald, https://www.herald.co.zw/digital-registry-services-to-start-by-december/ (accessed 20 November 2022).

The Demand for Digital Verification Rises across Africa, Digital Banker Africa, https://digitalbankerafrica.com/the-demand-for-digital-verification-rises-across-africa/ (accessed 22 March 2023).

Robert and Oloyede, Why Millions of Africans Are Right to Resist Mobile SIM Card Registration, Institute of Development Studies, https://www.ids.ac.uk/opinions/why-millions-of-africans-are-right-to-resist-mobile-sim-card-registration/ (accessed 20 November 2022).

Lagos to Launch Smart ID Card for Residents, Tribune Online, https://tribuneonlineng.com/lagos-to-launch-smart-id-card-for-residents/ (accessed 20 November 2022).

Our Servers Not Hacked, Remain Most Secure for Identity Management – NIMC, TVC News, https://www.tvcnews.tv/2022/01/our-servers-not-hacked-remain-most-secure-for-identity-management-nimc/ (accessed 20 November 2022).

Unlawful SIM Card Validation Exercise Is a Threat to Anonymity and Privacy, Unwanted Witness, https://www.unwantedwitness.org/unlawful-sim-card-validation-exercise-is-a-threat-to-anonymity-and-privacy/ (accessed 20 November 2022).

Ukpe, NIMC Debunks Reports of Breach of Its Database, Nairametrics, https://nairametrics.com/2020/12/24/nimc-debunks-reports-of-breach-of-its-database/ (accessed 20 November 2022);

The State of Identification Systems in Africa, World Bank, http://documents1.worldbank.org/curated/en/298651503551191964/pdf/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf (accessed 10 November 2022).

Inclusive and Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable, World Bank, https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable (accessed 19 November 2022).

Country Profiles Report, World Bank https://openknowledge.worldbank.org/bitstream/handle/10986/28310/119065-WP-ID4D-country-profiles-report-final-PUBLIC.pdf accessed (16 September 2022).

Zelalem, Ethiopia Digital ID Prompts Fears of Ethnic Profiling, Context.news, https://www.context.news/surveillance/ethiopia-digital-id-prompts-fears-of-ethnic-profiling (accessed 22 March 2023).

Victoria Oloni

Cross-Border Data Flows: Oiling the Wheel of the African Digital Economy

https://doi.org/10.1515/9783110797909-010

A Introduction

Cross-border data flows are a fundamental prerequisite to a functional international data economy which in turn is the key driver of the global digital economy. When you order a new book on Amazon or shoes on Ali Express, download an app from Google or Apple store, make payment for your music streaming app or stream your favourite show on Netflix, your personal data is transferred across multiple jurisdictions. This is because organisations use servers located across different countries for many reasons including increased speed, lower network traffic and cost.[1] It is almost impossible to disassociate international data transfers from the digital economy because data is the fuel upon which the digital economy thrives. Cross-border data flows facilitate media, entertainment, trade, medicine, financial services and all-around economic growth and development. According to the International Data Corporation, by the end of 2022, 65% of the global GDP will be digital, and from 2020 to 2023, investments in digital transformation would amount to over US$6,800,000,000,000 which equal to the GDP of France and Germany put together.[2]

Africa is not left out of the digital economy revolution. In a 2020 report, the International Finance Corporation projected that e-commerce will to boost Africa's economy US$712,000,000,000 by 2050, increasing its sector contribution to the continent's Gross Domestic Product (GDP) to 8.5%. Furthermore, depending on how much digital technology is used by businesses and the correct combination of regulatory measures, the internet economy has the potential to contribute up to US $180,000,000,000 to Africa's GDP by 2025.[3] Similarly, the June 2022 report of Endeavour Nigeria stated that the estimated size of the digital economy is about US $115,000,000,000 and is expected to be over US$712,000,000,000 by 2050. According to this report, between 2010 and 2019, more than 300,000,000 Africans acquired access to the internet and currently, 2 in 3 Africans use the internet.[4]

The possibility of new markets and tempting new pathways for digital startups and e-businesses have opened up with the ratification of the Africa Continen-

1 López-González, Hitchhiker's Guide to Cross-Border Data Flows, 2019, https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows/, (accessed 15 May 2023).

2 Zurich Insurance Groups, Cross-border data flows: Designing a global architecture for growth and innovation 2022, https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation, (accessed 15 May 2023), p 5.

3 International Finance Corporation, e-Conomy Africa 2020, https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2, (accessed 15 May 2023), p 11.

4 International Finance Corporation, e-Conomy Africa 2020, p 12.

tal Free Trade Area. It is important to state again that the amazing predictions for the African digital economy will remain just figures on paper if the continent does not optimize the movement of data across jurisdictions like it is trying to do with goods and services. It is therefore surprising that there is a 50/50 divide between African nations that have adopted data flow restrictions and those that had not. For example, 26 African nations have established conditional flow regimes, and 26 more have no limitations on cross-border data transfers. This paper attempts to juxtapose the rationale for both sides of the divide and proffer recommendations on improving cross-border data transfer within Africa for an improved and optimised African digital economy.

B Approaches to Cross-Border Transfer

The rapid digitalisation of the economy and the "datafication" of society have prompted governments around the world including in Africa to adopt different approaches to cross-border data flows. These different approaches have been grouped by scholars under 4 main categories:[5]

I No Regulation

At one extreme, there is no control of cross-border data flows in some jurisdictions (particularly in less developed nations / states), typically because there is no data protection legislation at all e.g Libya[6], Sudan.[7] Although this means that there are no constraints on the cross-border transfer of data, the lack of regulation might have an impact on other data subject's willingness to provide their personal data. On another hand, there may be a data protection law in existence, but this law does not contain specific provisions on cross-border transfer. In this instance,

5 López-González, Trade and cross-border data flows, OECD Going Digital Toolkit Notes, No. 11, OECD Publishing, Paris 2021, https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_7bc12916-en, p. 13.

6 Nevertheless, the Libya 2011 Constitution, specifically in Articles 12 and 13, prescribes that citizens have the right to privacy and confidentiality of their communications, including correspondence and telephonic conversations. Exceptions to this right are allowed only when a judicial warrant is issued.

7 UNCTAD, Data Protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed 07 August 2023).

save for requirements around further processing of personal data, there is no regulation for cross border transfer of data.

II Open Transfer Approach

Under this approach, there are no mandatory requirements and cross-border transfer is mostly regulated by private standards. This approach has been adopted by the United States of America, Canda, Australia etc and allows companies to send data across borders, and the companies are held accountable for how the personal data is processed. This approach does not impose any requirements on the transfer of data across borders, but it does provide for ex-post accountability for the data exporter when data sent abroad is misused.

III Conditional Transfer Approach

This appears to be the most favoured and widely used approach across the world. It was adopted by the European Union (the "EU") in the 1995 EU Data Protection Directive and subsequently the General Data Protection Regulation (the "GDPR") and is also used in African countries like Nigeria, Kenya and South Africa. In this approach, cross-border data transfer is regulated by regulatory safeguards. This approach typically relies on a finding of an adequacy level of protection as a condition for data transfer. In the absence of an adequacy decision, organisations can transfer data using appropriate safeguards like standard contractual clauses, binding corporate rules, ad hoc contracts etc. or derogations like consent or vital interest.

IV Limited Transfer Approach

This approach imposes strict requirements on cross-border data transfers. This approach may require case-by-case basis approval of data transfer requests by the relevant authorities and may also require that data is stored locally with strict conditions attached to cross-border transfer. For example, Russian Federal Law of 21 July 2014 No. 242-FZ (as amended) mandates that all personal data about Russian citizens must be stored and processed using databases physically located in Russia,

while allowing for cross-border transfers of copies of the data once this requirement is met.[8]

C The Legal Framework for Cross-Border Transfer in Ghana, Kenya, Nigeria, Rwanda, and South Africa

I Ghana

The Ghanaian Data Protection Act, which was passed into law in 2012, makes passing references to the transfer of data[9], but it does not provide for a comprehensive framework on this subject. Consequently, there is a scarcity of comprehensive literature addressing the topic of cross-border data transfers in Ghana, apart from a limited number of articles and reports.[10] It however appears that there is generally no statutory or regulatory aversion towards cross-border data transfer from government institutions.

II Kenya

The Kenya Data Protection Act (the "KDPA") has adopted the conditional transfer approach to the cross-border transfer of data from Kenya. When the draft Kenya Data Protection Bill was released for consultation in 2018, the Bill contained restrictions on cross-border data transfers.[11] Additionally, the processing of sensi-

8 OneTrust Data Guidance, Russia- Data Protection Overview, December 2022, https://www.dataguidance.com/notes/russia-data-protection-overview-0 (accessed 07 August 2023).

9 Section 47(1) of the Ghanaian Data Protection Act requires data controllers to provide information on countries the data controller may transfer data when applying from registration with the data protection authority. Section 18 (2) of the Ghanaian Data Protection Act also requires data controllers to process the data of foreign data subjects in compliance with data protection legislation of the foreign jurisdiction of that subject where personal data originating from that jurisdiction is sent to Ghana.

10 Hoffmann, Data Protection Act(ion) Report on the Law of Data Disclosure in Ghana see it at IRDG_Research_paper_Series_Country_Report_Ghana_Final.pdf (uni-passau.de), Dei-Tutu/Hoffmann, Assessing Ghana's Data Protection Framework within the Context of Africa's Data Governance Strategy: Trends, Direction and Prospects in Hennemann (ed) Global Data Strategies, Beck Verlag, 2023, p. 83.

11 Section 44 (1) of the Draft Data Protection Bill 2018.

tive personal data outside of Kenya was forbidden by the Bill.[12] These provisions were however contested by several stakeholders and did not make it to the final iteration of the Bill that was passed in 2019. The KDPA provides that data may be transferred outside Kenya only where certain conditions are met (proof of appropriate safeguards, performance of contractual obligations, public interest, vital interest, legitimate interest).[13] However, processing of sensitive personal data outside Kenya must be accompanied by the consent of the data subjects.[14] The KDPA also empowers the Cabinet Secretary to restrict the processing of data of a particular nature to servers or data centres located in Kenya on the grounds of strategic interests of the state or protection of revenue.[15]

III Nigeria

Cross-border transfer of data from Nigeria is generally governed by the Nigeria Data Protection Act 2023 (the "NDPA") and the Nigeria Data Protection Regulation 2019 (the "NDPR") along with certain sector-specific laws. Like in Kenya, the NDPA adopts a conditional transfer approach to cross border transfer of data. According to the NDPA, data can be transferred outside Nigeria where there is a determination of the adequacy of protection for the data in the recipient's country encompassing recipient laws, binding corporate rules, contractual clauses, a code of conduct or a certification mechanism; or (b) one of the conditions outlined in section 43 of the NDPA is present.[16] With regards to the adequacy prerequisite, the National Information Technology Development Agency ("NITDA"), in issuing the Implementation Framework for the NDPR in 2020 (the "Implementation Framework"), included a Whitelist of countries deemed to have adequate data protection laws

12 Section 44 (3) of the Draft Data Protection Bill 2018.
13 Section 48 of the Kenya Data Protection Act 2019.
14 Section 49 of the Kenya Data Protection Act 2019.
15 Section 50 of the Kenya Data Protection Act 2019.
16 The conditions outlined in the NDPA includes; (i) the data subject provides consent and understands the potential risks due to inadequate protection; (ii) the transfer is necessary for fulfilling a contract the data subject is involved in or taking steps requested by the data subject before entering into a contract; (iii) the transfer is solely for the benefit of the data subject and obtaining consent is not practically feasible, but it is likely the data subject would give consent if possible; (iv) the transfer is necessary for significant public interests; (v) the transfer is required for establishing, exercising, or defending legal claims; or (vi) the transfer is necessary to protect the vital interests of the data subject or other individuals, especially if the data subject is incapable of providing consent either physically or legally..

(the "Whitelist").[17] However, since the Implementation Framework was issued in November 2020, the Whitelist has not been updated

Although the NDPA and the NDPR do not contain data localisation requirements, some sector-specific guidelines/regulations restrict the cross-border transfer of certain categories of data from Nigeria. The National Cloud Computing Policy (version 1.2) August 2019 (the "Policy") classifies data into (a) Official, public or non-confidential data (Data of limited sensitivity); (b) Confidential, routine government business data (Data of moderate sensitivity); (c) secret, sensitive government and citizen data; and (d) classified or national security information. The Policy prescribes that (b) and (c) must reside primarily in a cloud framework within the Nigerian territorial boundary and (d) must reside only on-premises of the public institutions or collocated or in a cloud within the Nigerian territorial boundary.[18] The NITDA Guidelines for Nigerian content development in Information and Communication Technology (ICT) 2013 (the "Guidelines") also prescribe the local hosting of all sovereign data[19] in Nigeria and prohibit the transfer of sovereign data outside the shores of Nigeria without NITDA's express approval.[20] The Guidelines also require all ICT companies to host all subscriber and consumer data in Nigeria.[21] The Central Bank of Nigeria Guidelines on Point of Sale Card Acceptance Services prohibit the routing of transactions outside Nigeria for switching between Nigerian issuers and acquirers.[22]

IV Rwanda

The Rwanda Data Protection Law (the "RDPL") which was passed in 2021 also adopts the conditional transfer approach like Kenya and Nigeria. Under the RDPL, a data controller/processor may transfer personal data to another country only where certain conditions are met (authorisation from the supervisory authority, data subject consent, performance of contract, vital interest, compelling legitimate interest and performance of international instruments ratified by Rwanda).[23] In addition, the storage of personal data outside Rwanda is only permitted

17 Annexure C to the Implementation Framework.

18 Para 9.0 of the National Cloud Computing Policy.

19 Sovereign data in this sense means government data.

20 Guidelines 11.1(4), 12.1(4), 13.1(2), and 13.2(3), NITDA ICT Guidelines.

21 Guideline 12.1(4) of the Guidelines for Nigerian Content Development in Information and Communication Technology.

22 Guideline 4.4.8 POS Guidelines.

23 Article 48 of the Rwanda Data Protection Act.

if the data controller or the data processor holds a valid registration certificate issued by the supervisory authority authorising such storage.[24] The supervisory authority has also the power to prohibit or suspend the transfer of personal data outside Rwanda to protect the rights and freedoms of the data subject.[25]

V South Africa

Under the Protection of Personal Information Act (the "POPIA") regime, South Africa appears to adopt a conditional transfer approach to cross border transfer of data. However, in 2021, the Department of Communications and Digital Technologies published the Draft National Data and Cloud Policy (GG No. 44389) (the "Draft Policy") that introduces certain data localisation requirements. The Draft Policy outlines several key points regarding data management and ownership within South Africa. It mandates that all data classified as critical information infrastructure must be processed and stored within the country's borders.[26] Cross-border transfer of citizen data is allowed but must adhere to South African privacy protection policies, including POPIA and constitutional provisions, as well as international best practices.[27] Nothwithsatnding the above, a copy of such data must be stored in South Africa for law enforcement purposes.[28] The policy also emphasizes ownership and control, with data generated in South Africa considered the property of the country regardless of the technology company's domicile.[29] Although this policy is currently in a draft form and has not yet entered into force, there has been a lot of opposition to its adoption and subsequent execution of the Draft Policy's data localisation provisions.

24 Article 50 of the Rwanda Data Protection Act.
25 Article 49 of the Rwanda Data Protection Act.
26 Paragraph 10.4.1 of the Draft National Data and Cloud Policy.
27 Paragraph 10.4.2 of the Draft National Data and Cloud Policy.
28 Paragraph 10.4.3 of the Draft National Data and Cloud Policy.
29 Paragraph 10.4.4 of the Draft National Data and Cloud Policy.

D Africa Policy Framework: Cross Border Data Flows and the Digital Economy

I The AU Data Policy Framework 2022

The AU Policy Framework (the "Framework") presents a common vision, agreed principles and strategic priorities for the African Union. It also contains key recommendations to guide member states through the formulations of policy in their domestic context, as well as recommendations to strengthen cooperation among countries and promote intra-Africa flows of data. The Framework was endorsed by the AU Executive Council in February 2022. The Framework's guiding principles are cooperation, integration, fairness and inclusiveness, trust, safety and accountability, sovereignty, comprehensive and forward-looking, integrity and justice.[30]

Key Points and Recommendations

The key points and recommendations outlined in the Framework pertaining to cross-border data transfer are as follows: Firstly, the evaluation of data localization should consider its potential impact on human rights.[31] In addition, when deciding on a particular cross-border data protection approach, a delicate equilibrium must be maintained between advancing balanced economic growth and ensuring sufficient data security.[32] Data protection authorities are also encouraged to embrace international and regional collaboration practices while recognizing the varying degrees of implementation and enforcement across Member States.[33] Lastly, in formulating data localization strategies encompassing policy development, risk assessment and engagement with multiple stakeholders, inclusive of civil society participation, should be taken into account.[34]

30 Page 19 of the AU Data Policy Framework 2022.
31 Para 5.4.1.2 of the AU Africa Policy Framework.
32 Para 5.3.6.2 of the AU Africa Policy Framework.
33 Para 5.4.1.2 of the AU Africa Policy Framework.
34 Para 5.4.1.2 of the AU Africa Policy Framework.

II African Union Convention on Cyber Security and Personal Data Protection 2014 (Malabo Convention)

The Malabo Convention details the basic principles and guidelines for safeguarding personal data in Africa. Signatories to the convention are obligated to establish domestic policy measures that conform to the guidelines set out in the convention, to curtail and mitigate occurrences of cybercrime and privacy violations. It is interesting to note that the Malabo Convention follows the conditional transfer approach, with the transfer of personal data being permissible only where a state ensures that the level of protection of privacy, freedoms and fundamental rights of persons whose data are being or are likely to be processed is adequate.[35]It is noteworthy that the Malabo Convention only came into force in June 2023, after Mauritania's ratification of the conventin on May 9 2023.[36]

III The Personal Data Protection Guidelines for Africa 2018

The Internet Society and the African Union Commission joined forces to launch the Personal Data Protection Guidelines for Africa (the "Guidelines") on May 9 2018. Its major goal, as envisioned by the Malabo Convention, is to give African Union member states advice and information on how to ensure the security of personal data as well as regulatory approaches to data protection. The Guidelines refer to the principles established within the Malabo Convention. The Guidelines contain recommendations for stakeholders in different sectors including governments and policymakers, data controllers and processors and data protection authorities. These Guidelines also contain recommendations on themes like multi-stakeholder solutions, the well-being of the digital citizen, enabling and sustaining measures etc.

One of the key recommendations within the Guidelines is the establishment of Data Protetcon Authorities ("DPAs") by each member state signatory to the Malabo Convention. The DPAs should be independent bodies and should have members representing stakeholders (such as citizens, government, etc.) to carry out their functions and fulfil their objectives. It appears that the intention is to allow for

35 Article 14 (6) (a) of the Malabo Convention.

36 Yohannes Eneyew Ayalew, The African Union's Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?, 2023, https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/ (accessed 08 August 2023).

a more multi-faceted approach to data protection as a step towards secured cross-border data flows within the African continent.

IV The Digital Transformation Strategy for Africa (2020–2030)

The Digital Transformation Strategy for Africa (2020–2030) (the "Strategy") was developed by the African Union and issued on the 9 February 2020. The overall objective of the Strategy is "to harness digital technologies and innovation to transform African societies and economies to promote Africa's integration, generate inclusive economic growth, stimulate job creation, break the digital divide, eradicate poverty for the continent's socio-economic development and ensure Africa's ownership of modern tools of digital management".[37]

The Strategy outlines specific objectives of the African Union with respect to driving digital transformation, propelling industrialisation of the African digital economy. The Strategy builds on other frameworks on trade in Africa such as the African Continental Free Trade Area and the Policy and Regulation Initiative for Digital Africa ("PRIDA").

The Strategy encompasses several key objectives, including the establishment of a secure digital single market in Africa by 2030 in alignment with AfCFTA, the entry into force of the Malabo Convention by 2020, which wasn't met until June 2023, and the advocacy for open standards and interoperability to facilitate cross-border trust frameworks, personal data protection and privacy.[38] The Strategy also recommends collaboration among African institutions and regulators, the implementation of regulations and policies to ensure the confidentiality of patient personal data, thus fostering trust in digital health solutions as well as the adoption of national strategies, legal frameworks and standards for cybersecurity and data protection among others.[39]

V The Africa Continental Free Trade Agreement (AfCFTA)

The Africa Continental Free Trade Agreement ("AfCFTA" or the "Agreement") is the trade agreement established between fifty-five (55) countries in the African Union and 8 regional economic communities. Its purpose is to industrialise the African

37 Para II (B) of the Digital Transformation Strategy.
38 Para II (C) of the Digital Transformation Strategy.
39 Para VII of the Digital Transformation Strategy.

continent and boost economic integration between African countries. This includes economic relations and cross-border trading. Although the AfCFTA is not a data protection instrument, and does not contain express data protection provisions, Article 15(c)(ii) of the Protocol on Trade in Services recognises the preservation of individual privacy in connection to the processing and dissemination of personal data and the protection of the confidentiality of personal records and accounts as exceptions to trade restraints.

E Challenges to Cross-Border Data Flows in Africa

One of the biggest challenges to cross-border data flow in Africa is the spread of data localisation laws and policies. Data localisation has been defined as "the act of storing data on any device that is physically present inside the borders of the country where the data was generated."[40] It is a measure that specifically encumbers the movement of data across a nation's border.[41] Data localisation is also referred to as a regulation requiring companies to build computing facilities on the soil of the country where they are headquartered (localised data hosting).[42] It could also be understood as a government's explicit directive to internet service providers to limit data packet routing to inside-state boundaries (localised data routing).[43]

The spread of data localisation policies is not peculiar to the African continent. From 35 in 2017 to 62 in 2021 and 67 in 2017 to 144 in 2021, the number of nations with data localisation laws and the overall number of data localisation rules (including explicit and de facto) has nearly doubled.[44] The following section interrogates the justifications that have been put forward in support of data localisation and the (potential) impact of data localisation on the African digital economy.

40 Rouse, What Does Data Localization Mean?, 2017, https://www.techopedia.com/definition/32506/data-localization#:~:text=Data%20localization%20is%20the%20act,where%20the%20data%20was%20generated, (accessed 15 May 2023).

41 Chander and Lê, Data Nationalism, Emory Law Journal, vol. 64, 2015, p 678.

42 Bagchi and Kapilavai, Political Economy of Data Nationalism, presented at the 22nd Biennial Conference of the International Telecommunications Society, 2018, p 4.

43 Selby, Data Localization laws: trade barriers or legitimate responses to cybersecurity risks or both?, International Journal of Law and Information Technology, 2017, p 214.

44 Cory and Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, ITIF, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/, (accessed 15 May 2023).

I Justification for Data Localisation

1 National Security and Foreign Surveillance

Perhaps the strongest argument presented by the government in favour of data localisation is national security and protection from foreign sureveillance. There is widespread assumption that keeping personal information, emails and other types of data within the national boundaries would reduce foreign surveillance and safeguard residents' online privacy. It is feared that storing crucial personal data servers abroad will enable foreign governments to violate the privacy and security of such data. The advent of cyber terrorism and cyber espionage by state and non-state actors has increased concerns about the security of data held outside of a nation's borders, giving rise to what appears to be a valid concern for national security.

2 Law enforcement and Cybercrimes

Investigation into cybercrimes is typically challenging because the act might simultaneously cover several countries. It is assumed that storing data in a foreign country without providing access or capacity to domestic law enforcement may make it more difficult for such authorities to carry out their tasks. These difficulties can bring hardships to effectively investigate cybercrimes.[45] Data localisation is thus a simpler policy choice for some jurisdictions to safeguard law enforcement. The problem with this reasoning is that cybercrimes are multinational and cross-jurisdictional, rendering data localisation policies ineffective against cybercrimes.

3 Economic Development

Localising data within national boundaries is thought to boost local investment. The aforementioned practice is referred to as "Data mercantilism"[46], which is an open government policy to leverage data as a strategic asset to gain economic

45 Selby, Data Localization laws: trade barriers or legitimate responses to cybersecurity risks or both?, p 216.

46 ITIF, Localization Barriers to Trade: Threat to the Global Innovation, 2013, https://www2.itif.org/2013-localization-barriers-to-trade.pdf, (accessed 15 May 2023), p 18.

and political advantage. Azmeh and Foster[47] outlined the advantages of a data localisation policy for developing nations to include increased foreign direct investment in digital infrastructure and favourable spillover effects of a domestic market for data centres through improved connectivity, job creation and the presence of skilled professionals.[48]

4 Tax Benefits

Another justification that has been given for data localisation is that data localisation ensures that foreign corporations pay taxes on the revenue generated from processing citizens' data. By hosting servers locally, foreign companies are considered to have a "fixed place of business" and are therefore subject to taxation. This provides a strong justification for localising data.

This claim may, however, be rendered moot by policies of countries introducing the concept of significant economic presence to bring foreign companies under the local tax net. For example, in Nigeria, the Companies Income Tax (CIT) (Significant Economic Presence) Order 2020 (the "Order") in clarifying the provision of Section 13(2)(c) and (e) of the Companies Income Tax Act (CITA) provides that foreign companies qualify as having significant economic presence in Nigeria in any accounting year, where they derive ₦25,000,000 annual gross turnover or its equivalent in other currencies from any or combination of the digital activities listed in the Order. This order solves the concerns around the taxation of foreign entities without mandating the local storage and processing of personal data.

II The Impact of Data Localisation on the African Digital Economy

Although there are many compelling arguments in favour of data localisation, these advantages come at a hefty price. In 2019, Badran and Tufail published an economic impact assessment of data localisation in Egypt, Kenya, Mauritius, Morocco, and South Africa and found that cross-border data transfer restrictions

47 Azmeh and Foster, The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements, Working Paper Series 2016, https://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf, (accessed 15 May 2023), pp. 16 ff.

48 Agarwal, Data as a Tool for Diplomacy in India, JURIST, 2020, https://www.jurist.org/commentary/2020/05/akshat-agarwal-data-localization-india/ (accessed 15 May 2023).

would result in a real GDP decline for all the countries studied. Additionally, all countries would experience increases in production costs and a decline in income due to increases in the prices of goods.

1 Economic Impact

The European Centre for International Political Economy has found that localisation measures will cost nations like China, Indonesia, Brazil, India, and Vietnam between 0.2% and 1.7% of GDP and 0.5% to 4.2% in domestic investment.[49] Businesses may leave the country if they no longer believe that the cost of storing data locally is worthwhile given the advantages they receive. The study concluded that localisation restrictions cost EU citizens an estimated US$193,000,000,000 per year, in part because of increased domestic pricing, proving that even the European Union (EU) is not exempt.[50]

Another study estimates that the cost of domestically storing data in Nigeria will range from 0.2% to 4.2% of domestic investment.[51] These policies have a hefty price tag. Data localisation rules may ultimately have a negative impact on the economy and generally put countries with such policies at an economic disadvantage.

2 Organisational Cost

For consumers and enterprises, data localisation may result in higher business costs. Businesses, especially start-ups, depend on leasing or renting server capacity/data storage capacities from larger companies that are frequently located in foreign countries due to the high cost of local data storage. The implementation of data localisation policies will prevent these businesses from leveraging these cheaper models hence increasing the cost of business operations. The added expense will be passed on to customers to lessen the impact of the cost increase on the company, increasing the cost of services for consumers.[52]

---

49 Agarwal, Data as a Tool for Diplomacy in India.

50 Agarwal, Data as a Tool for Diplomacy in India.

51 Nwosu, Data Localization: The Effects on Cloud-Adoption in Nigeria, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3065432, (accessed 15 May 2023), p 5.

52 The Dialogue, Data Localization in A Globalised World: An Indian Perspective, 2018, https://thedialogue.co/wp-content/uploads/2020/01/Data-Globalisation-in-a-Globalised-World-copy_compressed.pdf, (accessed 15 May 2023), p 51.

3 Data Security

Data localisation may unintentionally increase the risk of security breaches since businesses will be compelled to work with regional service providers that might not offer the best security for their services making them easy targets for cyberattacks. For organisations, the physical centralisation of data poses a "jackpot" problem because a hacker only needs to compromise a small number of servers to have access to the data of its users. The mere fact that data is located within a certain jurisdiction does not automatically increase security. The technological, organisational and financial ability of an enterprise to safeguard data and provide physical security for a data centre are greater determinants for data security.

4 The Structure of the Internet

Data localisation undermines the open and interoperable internet architecture which goes against the original objective of internet creation from a technological standpoint. According to the Global Commission on Internet Governance's final report, data transmission on the internet adheres to the principle of efficiency and disregards border considerations.[53] According to the report, data localisation will "shake the stability of the internet infrastructure."[54] Data localisation policies, according to some authors, may also be incompatible with emerging information technology trends like big data, the Internet of Things (IoT) and cloud computing.[55]

5 Global Trade

Global trade depends on the free flow of data. The General Agreement on Trade in Services of the World Trade Organisation permits trade restrictions as long as they are necessary to protect people's privacy when it comes to the processing, sharing and confidentiality of their personal data[56], and as long as they do not amount to "arbitrary or unjustifiable" discrimination between nations or a covert restriction on trade and services. Similar provisions are contained in Article 15(c)(ii) of the

53 Global Commission on Internet Governance, One Internet: Final Report of the Global Commission on Internet Governance, 2016, https://www.cigionline.org/publications/one-internet/, (accessed 15 May 2023), p 36.

54 Global Commission on Internet Governance, One Internet, p 55.

55 Chander and Lê, Data Nationalism, p 728.

56 Article XIV (c) (ii) of the General Agreement on Trade in Services.

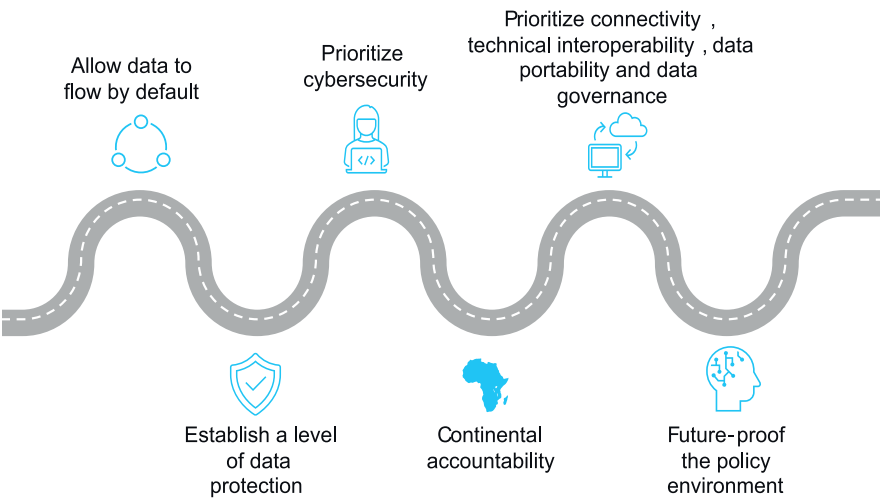

Fig. 1: Roadmap for Cross-Border Data Flows.

Protocol on Trade in Services of the AfCFTA. Strict adherence to data localisation guidelines could come out as "unjustifiably discriminatory" toward other nations. Although it may be necessary to restrict cross-border data transfers for privacy reasons, it might be difficult to implement such restrictions in a world that is becoming more interconnected.

One of the most important policy concerns for the African digital economy is the development of a strong, balanced strategy and appropriate regulatory frameworks for cross-border data movement among African nations. In developing this strategy, it is important to consider the following:

a) allowing data to flow by default within Africa;
b) prioritising cybersecurity;
c) promoting an agile framework to allow for innovation and experimentation;
d) ensuring accountability of all stakeholders within the data lifecycle;
e) establishing standards for data accuracy and quality; and
f) establishing and implementing an African data governance approach that takes into cognizance the peculiarities of the African continent.

It is important to ensure that the African data governance approach is not too watered down or different from globally acceptable standards. This is because Africa cannot as a continent function in isolation and whatever approach is adopted should be able to encourage and facilitate cross-border data flows beyond Africa.

F Conclusion

In conclusion, cross-border data flows play a crucial role in facilitating the growth of the African digital economy and the introduction of data localisation policy may have an adverse effect on the growth of the African digital economy. While there are justifications for localising data, it is important to strike a balance between privacy concerns and promoting innovation and economic growth. African countries should adopt a harmonised policy framework to ensure that data transfer regulations do not hinder the development of the digital economy. The roadmap for cross-border data flows should prioritise addressing the challenges and fostering a conducive environment for cross-border data transfer. Ultimately, promoting cross-border data flows in Africa will require collaboration among stakeholders, including governments, private sector players and civil society.

G Bibliography

Agarwal, Data as a Tool for Diplomacy in India, JURIST, 2020, https://www.jurist.org/commentary/2020/05/akshat-agarwal-data-localization-india/, (accessed 15 May 2023).

Azmeh and Foster, The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements, Working Paper Series 2016, 2016, https://www.lse.ac.uk/international-development/Assets/Documents/PDFs/Working-Papers/WP175.pdf, (accessed 15 May 2023).

Bagchi and Kapilavai, Political Economy of Data Nationalism, the 22nd Biennial Conference of the International Telecommunications Society: "Beyond the boundaries: Challenges for business, policy and society", Seoul, 2018.

Chander and Lê, Data Nationalism, Emory Law Journal, vol. 64, 2015.

Cory and Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, ITIF, 2021, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/, (accessed 15 May 2023).

ECIPE, The costs of Data Localisation: friendly fire on economic recovery, 2014, https://ecipe.org/publications/dataloc/, (accessed 15 May 2023).

Irfan, Data Flows, Data Localisation, Source Code: Issues, Regulations and Trade Agreements. Geneva: CUTS International, Geneva, 2019.

International Finance Corporation, e-Conomy Africa 2020, https://www.ifc.org/wps/wcm/connect/e358c23f-afe3-49c5-a509-034257688580/e-Conomy-Africa-2020.pdf?MOD=AJPERES&CVID=nmuGYF2, (accessed 15 May 2023).

ITIF, Localization Barriers to Trade: Threat to the Global Innovation, 2013, https://www2.itif.org/2013-localization-barriers-to-trade.pdf, (accessed 15 May 2023).

López-González, Hitchhiker's Guide to Cross-Border Data Flows, 2019, https://www.oecd.org/trade/hitchhikers-guide-cross-border-data-flows/, (accessed 15 May 2023).

López-González, Trade and cross-border data flows, OECD Going Digital Toolkit Notes, No. 11, OECD Publishing, Paris 2021, https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_7bc12916-en, (accessed 15 May 2023).

Nwosu, Data Localization: The Effects on Cloud-Adoption in Nigeria, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3065432, (accessed 15 May 2023).

Rouse, What Does Data Localization Mean?, 2017, https://www.techopedia.com/definition/32506/data-localization#:~:text=Data%20localization%20is%20the%20act,where%20the%20data%20was%20generated, (accessed 15 May 2023).

Selby, Data Localisation laws: trade barriers or legitimate responses to cybersecurity risks or both?, International Journal of Law and Information Technology, vol. 25, 2017.

Zurich Insurance Groups, Cross-border data flows: Designing a global architecture for growth and innovation 2022, https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation, (accessed 15 May 2023).

Melody Musoni

The Role of Data Localisation in Cybercrime Investigations

A Introduction

In the global and interconnected world, data are indispensable. Importantly, the sharing of data between service providers and customers in different countries is the backbone of international trade.[1] The COVID-19 pandemic has facilitated

Note: Work on this chapter contains some discussions extracted from my Ph.D thesis titled "Legal challenges of establishing jurisdiction over cloud data: Addressing the gaps in South Africa's cybercrime legislative framework", Witwatersrand University, 2023.

1 Recital 101 of the General Data Protection Regulation recognises that transborder data flows outside the EU are necessary for the expansion of international trade and international cooperation.

https://doi.org/10.1515/9783110797909-011

the growth in digital trade and cross border data flows even when global GDP growth rates plummeted.[2] With cloud computing technologies, cross border data transfers are crucial not only for international trade but for investigation of crimes.[3] When data are hosted on servers in a foreign territory, law enforcement agents need to obtain necessary authorisations from the foreign state before they can exercise any enforcement powers over the data. Similarly, in instances where the sought-after data are under the control of a service provider, the law enforcement agent still needs necessary approvals before the service provider can provide access or disclose the data. The necessary approvals are usually in the form of mutual legal assistance treaties (MLATs) or executive agreements concluded between states. One of the notable challenges is that the process to execute such agreements is very slow[4] which may result in investigating states being frustrated in failing to timeously investigate and prosecute crimes.

To avoid these hurdles, states may resort to implementing data localisation measures with the aim of making data easily accessible for law enforcement purposes.[5] Criminal justice interests have motivated a lot of countries to adopt data localisation laws.[6] When data or copies of data are locally hosted, governments can demand disclosure of such electronic evidence without regard to foreign substantive rules and procedural standards.[7] This is because states can exercise enforcement jurisdiction over local data infrastructure. In such instances, states do not need to seek permission from a foreign state or wait prolonged periods for such a request to be processed.

This contribution discusses the different legal and policy interventions on data localisation adopted by African countries. It highlights why countries implement data localisation measures to assist law enforcement agents for purposes of

---

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 flow of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2 Kugler, The impact of data localisation laws on trade in Africa, Mandela Institute Policy Brief 08, 2021, p 1 (1).

3 Brehmer, Data localization: The unintended consequences of privacy litigation, American University Law Review, 2018, p 927 (944).

4 Daskal, Access to data across borders: The critical role for Congress to play now, Advance: The Journal of the ACS Issue Briefs, 2017, p 45 (47).

5 Woods, Against Data Exceptionalism, Stanford Law Review, vol. 68, 2016, p 729 (751).

6 Daskal, Privacy and security across borders, Yale Law Journal Forum, 2018–2019, p 1029 (1047).

7 There are three consequences for slow mutual legal assistance systems. First, states may resort to unilateral extraterritorial assertion of compulsory disclosure obligations. Second, states may pursue expanded hacking or broad decryption mandates. Third, states may resort to data localisation measures. Daskal, Advance: The Journal of the ACS Issue Briefs, 2017, p 45 (47).

crime investigation. It further highlights the ineffectiveness of data localisation measures and provides alternative solutions for law enforcement to access electronic evidence.

B What is Data Localisation?

There are different restrictions or barriers to cross border data flows such as data residency requirements that confine data within a country's borders. Policy conversations regarding data on the African continent have frequently centred on localisation as a governance mechanism.[8] In 2021, about 62 countries had adopted data localisation requirements and 144 countries had adopted data localisation requirements.[9] States consider data localisation measures as justifiable.[10] Data localisation measures are aimed at controlling national digital borders. Such measures vary from the imposition of restrictions on transfer of data to other countries to mandatory requirements to store data on local servers or keeping copies of data locally.[11] Fraser defines data localisation as the laws or measures put in place by governments which encumber the movement of data across national borders, or limit where and by whom they are stored or processed.[12]

I Strict data localisation

Ferracane identifies two types of restrictions to cross border data flows. The first one is strict restriction where there is a blanket ban on transferring of data abroad or a requirement for local storage or processing of data.[13] These restrictions can manifest in the form of policy, standards, laws and regulations. Data localisation measures aimed at local storage requirements can either be general or industry specific: Some measures can make it mandatory for any form of data to be locally

8 Razzano, Data localisation in South Africa: Missteps in the valuing of data, Mandela Institute Policy Brief 06, 2021, p 1 (5).

9 Kugler, Mandela Institute Policy Brief 08, 2021, p 1 (1).

10 Zheng, Comparative study on the legal regulation of a cross border flow of personal data and its inspiration to China, Frontiers of Law in China, 2020, p 280 (286).

11 Flaig, Lopez-Gonzalez, Messent and Jouanjean, Modelling data localisation measures, 19th Annual Conference on Global Economic Analysis, 2016, p 1 (1).

12 Fraser, Data localisation and the balkanisation of the internet, SCRIPTed: A Journal of Law, Technology and Society, 2016, p 359 (360).

13 Bailey and Parsheera, Data localisation in India: Questioning the means and ends, National Institute of Public Finance and Policy, 2018.

stored or processed, while others may focus on specific industry such as finance, telecommunications, health or the public sector.[14] For example, Nigeria's Guidelines for Content Development in ICTs strictly prohibits all government data and all subscriber and consumer data held by telecommunications companies from being transferred outside the country.[15] These measures were adopted to promote local content and increase domestic value in ICT products and services. Nigeria has also specific data localisation regulations applicable to the financial sector. In 2011, the Guidelines on Point-of-Sale Card Acceptance Services were issued by the Central Bank of Nigeria. In terms of these Guidelines, all domestic transactions had to use local switch services and switching between Nigerian Issuers and Acquirers cannot be done outside Nigeria.[16] Similarly, strict data localisation measures have been introduced through some data protection laws. For instance, section 70 of Zambia's Data Protection Act[17] provides as follows –

> … (1) A data controller shall process and store personal data on a server or data centre located in the Republic. (2) Despite subsection (1), the Minister may prescribe categories of personal data that may be stored outside the Republic. (3) Despite subsection (2), sensitive personal data shall be processed and stored in a server or data centre located in the Republic.

In South Africa, there are no strict data localisation requirements. However, the recently published draft National Data and Cloud Policy (NDCP)[18] will result in strict data localisation if its policy provisions are adopted in their current form.[19] Some of the objectives of the NDCP are to create an enabling environment for the provision of data and cloud services to ensure socio-economic development for inclusivity, promote connectivity and access to data and cloud services, remove regulatory barriers and enable competition, ensure implementation of effective cybersecurity, privacy and data and cloud infrastructure protection measures.[20]

---

14 Flaig, Lopez-Gonzalez, Messent and Jouanjean, 19th Annual Conference on Global Economic Analysis, 2016, p 1 (7).

15 Guideline 12.1.(4) of the Guidelines for Nigerian Content Development in Information and Communication Technology (ICT) 2013. The guidelines were established by Nigeria's National Information Technology Development Agency (NITDA).

16 Nigeria's Guideline 4.4.8. Guidelines on Point of Sale Card Acceptance Services, 2011.

17 Zambia Data Protection Act 3 of 2021.

18 National Data and Cloud Policy GN306 GG 44389 of 1 April 2021.

19 The NDCP provides a sense of the direction the South African government potentially intends to follow in the future. Beyleveld, Data localisation in Kenya, Nigeria and South Africa: Regulatory frameworks, economic implications and foreign direct investment, Mandela Institute Policy Brief 01, 2021, p 1 (3).

20 NDCP at 10.

The NDCP contains strict data localisation measures in respect of critical information infrastructure and data generated from South African natural resources. Policy intervention 10.4.1. provides that 'all data classified/identified as critical information infrastructure shall be processed and stored within the borders of South Africa'. This means that no international transfers are permitted in respect of critical information infrastructure data.[21] The NDCP proposes the establishment of the High-Performance Computing and Data Processing Centre (HPCDPC) within South Africa to process and maintain the high volumes of data facilities and cloud computing capacity and to consolidate existing public funded data centres.[22]

II Conditional data localisation

The second type of data localisation requirements or measures allow transfer or processing of data outside a country under clearly defined conditions.[23] This is also the case in laws without express data localisation requirements but imposes conditions for cross border data transfers, i.e *de facto* data localisation.[24] Conditional data localisation measures are prevalent in data protection laws[25], in so far as laws create barriers to cross border data transfers to an extent that they are effectively data localisation requirements.[26] Most data protection laws have conditional data localisation provisions[27] and cross border transfer of personal data is only permissible subject to complying with those conditions.[28] Compliance with these conditions can at times be very costly to the extent that some entities are forced to store data locally by default.[29]

The General Data Protection Regulation (GDPR) is a typical example of a data protection law whose complicated data transfer requirements result in a *de facto*

21 NDCP Policy intervention 10.4.1 at 27.

22 Policy intervention 10.1.3. NDCP at 20.

23 Gonzalez, Casalini and Porras, OECD Trade Policy Paper, 2022, p 1 (6).

24 Sheppard, Yayboke and Ramos, Center for Strategic & International Studies, 2021.

25 Wu, Sovereignty and data localization, The Cyber Project Harvard Kennedy School, 2021, p 1 (13).

26 Bauer, Lee-Makiyama, Van Der Marel and Verschelde, The costs of data localisation: Friendly fire on economic recovery, European Centre for International Political Economy Occasional Paper No. 3, 2014, p 1 (3).

27 Kugler, Mandela Institute Policy Brief 08, 2021, p 1 (1). Van der Berg, Data protection in South Africa: The potential impact of data localisation on South Africa's project of sustainable development, Mandela Institute Policy Brief 02, 2021, p 1 (4).

28 Bailey and Parsheera, National Institute of Public Finance and Policy, 2018.

29 Kugler, Mandela Institute Policy Brief 08, 2021, p 1 (1).

localisation framework.[30] Chapter V of the GDPR contains a list of conditions on cross border transfer of data. The GDPR permits international data transfers based on an adequacy decision.[31] For the EU Commission to pass an adequacy decision, it considers a variety of factors which include whether a foreign state respects human rights and fundamental freedoms. Importantly, the EU Commission assesses the "essential equivalence" (in relation to EU law) of foreign states' legislation such as criminal law, the ability of public authorities to access personal information, effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.[32] In addition, cross border transfers of personal data under the GDPR are also permitted if there are appropriate safeguards.[33] Appropriate safeguards may be provided for by a legally binding and enforceable instrument between public authorities or bodies, binding corporate rules (BCR), standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority and approved by the Commission, approved codes of conduct or approved certification mechanism.[34] Apart from relying on the adequacy decisions and appropriate safeguards, Article 49 of the GDPR also permits transborder flow of personal data under specific situations.[35]

30 Cory and Dascoli, How barriers to cross-border data flows are spreading globally, what they cost, and how to address them, Information Technology and Innovation Foundation, 2021, p 1 (4).
31 GDPR Article 45.
32 GDPR Article 45 (2) (a).
33 GDPR Article 46.
34 GDPR Article 46 (2).
35 Article 49 of the GDPR provides that in the absence of an adequacy decision pursuant to Article 45 (3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

a. The data subject has provided their explicit consent after having been informed of the possible risks of such transfers for the data subject.

b. The transborder transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.

c. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.

d. The transfer is necessary for important public interest.

e. The transfer is necessary for the establishment, exercise or defence of legal claims.

f. The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

g. The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that

South Africa's data protection law, the Protection of Personal Information Act (POPIA)[36], contains a list of conditions which must be met before any personal information is transferred across its borders. These conditions include a consent from the data subject[37], or the transfer being necessary for the performance[38] or conclusion of a contract[39], or the transfer is for the benefit of the data subject[40] or the third party recipient is subjected to a law, or existence of BCRs or binding agreement which provides adequate level of protection that effectively upholds POPIA principles.[41] If any of the provisions set out under section 72 of POPIA are met, personal data may be transferred outside of South Africa. The conditional flow of data under POPIA has been considered a balanced and moderate approach[42] which aligns with the African Charter of Human and Peoples Rights (ACHPR), the Declaration of Principles on Freedom of Expression and Access to Information and the UN High Commissioner for Human Rights necessity criteria.[43] The criteria for data transfers is that the recipient jurisdictions should at least guarantee international law human rights standards and strict data localisation measures should be avoided.[44]

To sum up, data protection laws set conditions which must be met before data can be transferred to another territory. If such conditions cannot be met, data will not be permitted to leave the territory, hence *de facto* data localisation.

III Open transfers regime / soft localisation

The opposite of strict data localisation measures is an open transfer regime. In terms of this regime, there is a minimum regulatory burden to the movement of

---

the conditions laid by the EU or EU member state law for consultation are fulfilled in the particular case.

36 The Protection of Personal Information Act, 4 of 2013 (POPIA).

37 Section 72 (1) (b) of POPIA.

38 Section 72 (1) (c) of POPIA.

39 Section 72 (1) (d) of POPIA.

40 Section 72 (1) (e) of POPIA.

41 Section 72 (1) (a) of POPIA.

42 Van der Berg, Mandela Institute Policy Brief 02, 2021, p 11.

43 Adeleke, Exploring policy trade-offs for data localisation in South Africa, Kenya and Nigeria, Mandela Institute Policy Brief 09, 2021, p 1 (3).

44 United Nations High Commissioner for Human Rights, The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, Human Rights Council Thirty-ninth session, A/HRC/39/29, para 32.

data and data can generally be transferred abroad with only some specific or minimal requirements for mandatory or conditional data localisation.[45] A good example of a data protection framework with open transfers is Ghana's Data Protection Act[46] which does not prohibit any cross-border data flows of personal data but requires foreign recipients to (not enforceable) comply with its provisions.[47]

Gonzalez *et al* points out that there is a new category of data localisation emerging. In terms of this approach, states do not require local storage of data. However, service providers are required to guarantee access to data when required by regulators, thus providing at least some cross-border controllability without hindering data flows. This new form of localisation is prevalent in Mexico and New Zealand.[48] The risk with this approach is that companies may adopt vastly different standards for different jurisdictions and without guaranteeing any minimum standards for personal data protection.[49]

C Why Do African Governments Enforce Data Localisation Measures?

I Data localisation supports local law enforcement interests

One of the cited reasons for the adoption of data localisation measures is the serving of law enforcement interests especially when investigating crimes. For instance, South Africa's NDCP advocates for copies of data to be stored in South Africa for purposes of law enforcement.[50] In terms of international law, a foreign enforcement agency seeking to access remotely based evidence need to follow the available channels for assistance instead of acting unilaterally. If foreign governments are not forthcoming in cooperating with the investigating state, this can delay the investigation process. In the case of evidence hosted in foreign based cloud data, a state shall not unilaterally access the remote cloud data. To access

45 Gonzalez, Casalini and Porras, OECD Trade Policy Paper, 2022, p 1 (6).

46 Ghana Data Protection Act 843 of 2012.

47 Hoffmann, Data Protection Act(ion), IRDG 22(01), p. 12.

48 Mexico's Federal Telecommunications Law requires data to be made available for 12 months, without stipulating that it must be stored in Mexico. New Zealand's data retention regulation for business records allows for data to be stored outside New Zealand provided it meets certain data integrity and access criteria. Gonzalez, Casalini and Porras, OECD Trade Policy Paper, 2022, p 1 (8).

49 African Union Data Policy Framework 2022 at 42.

50 NDCP at 27.

the data, the state will have to get permission through channels provided by means of mutual legal assistance treaties (MLATs). Unfortunately, processes for MLAT channels are very slow. The danger with snail-paced MLAT processes is they are likely to result in miscarriage of justice as criminals may get rid of or encrypt evidence while law enforcement is still waiting for approval from a foreign state. Data localisation therefore makes the processes of gathering electronic evidence for criminal investigations fast and efficient. This section discusses the features of the cloud and how they may hinder crime investigations. This discussion highlights the role of data localisation in law enforcement efforts.

1 Data divisibility and fragmentation

Cloud computing services mainly focus on ensuring efficiency as well as information security. Fragmentation of data is one of the unique features of cloud services which is aimed at ensuring efficiency. Fragmentation is also called sharding or partitioning.[51] It means that 'certain sets of data are split and distributed (in pieces) among various computers and automatically relocated depending on the supply and demand of storage space in the cloud at a certain point in time'.[52] The various computers to which fragments of the data are distributed can potentially be in different countries. When a user wishes to access the data, they do not access the data in fragments. Upon entering correct credentials, the fragmented data sets are automatically reunited, and the user will be able to access the full set of data seamlessly.[53]

Koops and Goodwin argue that the distributed, dynamic, and redundant nature of cloud storage makes it difficult to say 'where' a certain file 'is' when it is stored in the cloud. This is because 'it can be in multiple places simultaneously and still not be in any single place in its entirety'.[54] If data are divided and randomly scattered on data servers around the world, the challenge then is to identify the

51 Hon et al defines sharding as an automated procedure performed by a cloud provider's software, which automatically breaks data up into fragments for storage in different storage equipment, possibly in different locations, based on the provider's sharding policies, such as performance maximisation. 28. Hon, Millard and Walden, The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing, International Data Privacy Law, 2011, p 211 (213).

52 Koops and Goodwin, Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law, Tilburg Law School Legal Studies Research Paper Series, 2014, p 1 (22).

53 Ibid.

54 Ibid.

state with jurisdiction over the cloud data. Ordinarily, the country where the data centres are established has jurisdiction over the cloud infrastructure. However, it is unclear whether the state can exercise jurisdiction if the hosted data are for a foreign based user or owner even though some legislation commands this jurisdiction, such as Art. 3 (2) GDPR or Art. 45 (c) Data Protection Act of Ghana. Data localisation measures resolve these jurisdictional challenges as the investigating state is able to exercise authority over any data if they are obligatorily hosted on local servers and data centres.

2 Location independence

Some governments prefer localisation of data or traditional IT infrastructure as a way of preventing any persons outside the country from unilaterally accessing the data or remotely manipulating the data.[55] This stems from their understanding of cloud data location independence. Location independence means that cloud data can be accessed from an arbitrary location and not necessarily near the user.[56] If cloud data can be remotely accessed, there is a legitimate concern that foreign actors can access critical information or critical assets of a government. This is considered a legitimate concern for national security interests. To avoid this, some governments insist on localisation of data by means of establishing local IT infrastructure.

3 Data mirrors and data in transit

Law enforcement agents need to identify a perpetrator and the place where the crime occurred to investigate and successfully prosecute a criminal. Part of the investigation process involves gathering evidence which may be stored in the cloud. To gather the evidence, the LEA would also need to know the place or the location where the evidence is in order to secure relevant search warrant. This process of identifying the location of the sought-after evidence may be a difficult task for law enforcement. Most cloud service providers operate replica data centres. Cloud service providers build or rent out extensive pieces of land across the world to operate expansive server parks or data farms.[57] This is done so that in the event of a

55 Daskal, Vanderbilt Law Review, 2018, p 179 (220).
56 Daskal, The Yale Law Journal, 2015, p 125 (373).
57 Koops and Goodwin, Tilburg Law School Legal Studies Research Paper Series, 2014, p 1 (22).

server park malfunction, disaster or cyberattack, data may still be retrieved from the replica data centre. When data are in transit, its location may be difficult to ascertain. What this means for law enforcement is that they cannot get a search warrant from court, as the location of the evidence requirement cannot be sufficiently identified. This can be a constant hurdle for law enforcement since data are constantly moved around different servers subject to potentially different jurisdictions. Data localisation therefore presents a solution to this challenge.

4 Data mobility and loss of knowledge of location of data

Data can move at nearly the speed of light, in an unpredictable fashion and generally unknown to both the data subject and the governments seeking to access such data. While one may access their email message, it is not always possible to tell exactly where the data representing the email message might be located, as data are constantly moved around servers. Even cloud providers may not know where the sought-after data are located.[58] If the location of data is unknown, law enforcement cannot blindly conduct searches and seizures. To do so would likely threaten the sovereign interests of a foreign state, where the sought-after data happen to be located. Without knowledge of location of data, mutual legal assistance may not be feasible. The investigating state will not know which country to approach for legal assistance and cooperation. This can hamper law enforcement efforts.

II Data localisation and national security interests

The way data are collected, used, stored and transferred can have a material impact on national security, industry growth, geopolitical relationships and civil society.[59] National security interests are one of the commonly cited reasons for adoption of data localisation measures. However, what entails national security may differ from one state to the other. It is argued that the free flow of data to hostile or authoritarian regimes threatens the national security of their geopolitical adversaries. Without clear definitions for national security interests and data localisation, governments have an opportunity to argue for stronger data localisation man-

58 Dan Jerker B Svantesson, Internet & Jurisdiction Global Status Report 2019, Internet & Jurisdiction Policy Network, 2019, p 1 (31).

59 Wu, The Cyber Project Harvard Kennedy School, 2021, p 1.

dates.[60] Some countries are concerned about the consequences of hosting their data in foreign data servers in instances of severed diplomatic relations with a government hosting their data.[61] There is also a danger that authoritarian governments can use data localisation as a tool to limit democracy and human rights. This includes the infringement and violation of freedom of movement, the right to speak freely and express political dissent, and the right to personal privacy as well as overall control over people.[62]

III To re-gain sovereignty over data

Data sovereignty is still a nebulous term.[63] Scholars have varying views on how to define data sovereignty. Some define data sovereignty as the highest jurisdiction over all data produced by individuals, enterprises and related organisations within the jurisdiction of a country.[64] Data sovereignty is also seen as the extension of the sovereign authority that a state enjoys over its territory into the digital world.[65] This sovereign authority is defined by the state having autonomy and freedom to regulate data in line with its policies and laws.[66] It also extends to the power of a state to put in place laws, practices and customs on how data are to be processed.[67] Data sovereignty may extend to the authority that a state has, not only over the data or data infrastructure, but the people and entities who use the data and data infrastructure.[68] Simply put, data sovereignty is the effort by a state to exercise control over data and its flow.[69]

---

60 Sheppard, Yayboke and Ramos, Center for Strategic & International Studies, 2021, p 1 (6).

61 Resha, Addressing the potential for African digital governance to facilitate inclusive development: rights, rules & revenues, Discussion Paper, 2021, p 1 (7).

62 Sheppard, Yayboke and Ramos, Center for Strategic & International Studies, 2021, p 1 (6).

63 Celestine, Cloudy skies, bright futures: In defense of a private regulatory scheme for policing cloud computing, University of Illinois Journal of Law, Technology & Policy, 2013, p 141 (148).

64 Zheng, Frontiers of Law in China, 2020, p 280 (286).

65 Jong-Chen, Data sovereignty, cybersecurity, and challenges for globalization, Georgetown Journal of International Affairs, 2015, p 112 (112). While discussing rights of indigenous people, Tsosie defined data sovereignty as the right of a nation to govern the collection, ownership and application of data concerning the tribe or its members and to control data that is housed within tribal territory. Tsosie, Tribal data governance and informational privacy: Constructing indigenous data sovereignty, Montana Law Review, 2019, p 229 (230).

66 Zheng, Frontiers of Law in China, 2020, p 280 (286).

67 Ibid.

68 Goldsmith, Sovereign difference and sovereign deference on the internet, Yale Law Journal Forum, 2018–2019, p 818 (818).

69 Razzano, Mandela Institute Policy Brief 06, 2021, p 1 (5).

The South African government is one of the governments attempting to gain sovereignty over data. One of the objectives of the NDCP is 'to strengthen the capacity of the State to deliver services to its citizens, ensure informed policy development based on data analytics, as well as promote South Africa's data sovereignty and the security thereof'.[70] The South African government is aware of the dominance of foreign big technology companies on the African continent and concerned about how South Africa and Africa are unequal participants in data centres.[71] With the 'scramble for data' or 'data imperialism', South Africa, like most states, is rushing to establish its dominance in the data economy. The NDCP notes that the development and growth of the digital economy makes it necessary for South Africa to restrict and protect some of its citizens' data to effectively participate in the global digital economy.[72]

Simply put, governments want to have a strategic advantage over data produced within their territories in face of competition from other governments. At the same time, governments employ data localisation measures as protectionist measures. Governments are realising that their power is diminishing in the digital age[73] due to the growth in market share by major multinational technology companies and the rise of global multi-stakeholderist structures. Most data centres and cloud services are under the control of foreign entities.[74] Chinese owned companies like Baidu, Alibaba, Tencent and Xiaomi (BATX) as well as US owned companies like Google, Amazon, Facebook, Apple, and Microsoft (GAFAM) have significant presence on the African data centre market. Either these foreign companies invest (directly or through local entities) in data centres on the African continent, or they host African data on data centres outside Africa.[75] Data centre capacity is also not evenly distributed on the African continent and data centre infrastructure in Africa still lags leading markets. There are nearly 50 data centres in Africa, five in Kenya, eleven in Nigeria, five in Morocco and twenty-five in South

70 NDCP at 8.

71 NDCP at 25.

72 NDCP at 27.

73 Woods, Litigating data sovereignty, Yale Law Journal, 2018, p 328 (358).

74 Ibid.

75 A US entity acquired a stake in Teraco which owns Africa's largest data centres. Actis launched pan-African data centres in countries like Nigeria. Africa Infrastructure Investment Managers private equity firm acquired a majority of stake in Ngoya Etix DC, a carrier-neutral data centre located in Ghana. Liquid Intelligent Technologies recorded an influx in investor interest including from the US government's International Development Finance Corporation. Digital Council Africa, Africa Digital Infrastructure Market Analysis 2021 Report, https://www.wcoesarpsg.org/wp-content/uploads/2021/11/juanita-clark-africas-evolving-digital-landscape.pdf (accessed 11 May 2023).

Africa.[76] There are 643 technology hubs on the African continent and the growth forecast in cloud and data centre capacity is up to 80 per cent.[77] African governments believe that data localisation requirements will help them re-gain their data sovereignty and have autonomy to decide for themselves how to regulate their digital infrastructure and how to plan for their digital futures.[78]

Technology companies exercise monopoly over data hence allow them to capture political power. The NDCP highlights the challenge of freemium business models which allows technology companies to collect unlimited amounts of data from African customers and subsequently sell the data globally for advertising purposes.[79] Some governments fear being digitally colonised and excluded from the digital economy by either foreign governments or by multinational corporations dominating the data market.[80] There are arguments that data about people in Africa should remain in Africa and African states should have autonomy to decide for themselves how to regulate their digital infrastructure and how to plan their digital futures.[81]

IV Protection of the right to privacy and security of citizens data

States also and maybe foremost justify the adoption of data localisation measures to protect their citizens' fundamental human rights. This justification is eminent in data protection laws. The Institute of International Finance noted that the objectives of data localisation measures, including security, privacy and inclusive sustainable economic growth are worthy of pursuit.[82] Kuner argues that data nationalism measures particularly on data protection are meant to protect the rights to

76 Resha, Discussion Paper, 2021, p 1.

77 An interactive view of cloud computing in Africa 2021, International Finance, 25 January 2021, https://internationalfinance.com/an-interactive-view-of-cloud-computing-in-africa/ (accessed 02 October 2022). See also The Africa Digital Infrastructure Market Analysis 2021 Report. Where it is estimated that data centres serving 1,26 billion people in Africa is about 140,000 square meters which is the same amount of data centre space serving Switzerland's 8,5 million people.

78 AU Data Policy Framework 2022.

79 NDCP at 26.

80 Van der Berg, Mandela Institute Policy Brief 02, 2021, p 1 (5–6).

81 Hofmann Towards an African narrative on digital sovereignty, 2022, https://www.hiig.de/en/african-digital-sovereignty/#:~:text=Data%20about%20people%20in%20Africa,to%20plan%20their%20digital%20futures (accessed 11 May 2023).

82 Institute of International Finance (IIF).

privacy and not as a protectionist measure[83] such as to protect domestic business interests from international competition. When data are stored abroad, there are legitimate concerns relating to the privacy interests of the owners of the data. There are concerns that many organisations collect, process and store massive amounts of data but lack security and privacy protections.[84] This argument emanates from the lack of robust data protection laws in other jurisdictions. The absence of effective data protection laws means that foreign based data can easily be accessed by foreign governments. As mentioned earlier, some countries view data localisation as critical to protecting their respective citizens from foreign surveillance[85] mainly from the US government.[86] What the Edward Snowden revelations highlight is that the US carries out mass surveillance on foreign governments and foreign citizens.

Generally, most states can protect fundamental human rights if they have control over the data and the persons accessing the data. When foreign states access data, data subjects often do not enjoy the protection of constitutional or other (national) human rights legislation in the surveilling country.[87] If a third country accesses data and any privacy infringement occurs outside the state of origin, the latter is incapacitated from exerting its authority over the data breach. This leaves citizens data vulnerable. The other notable justification for data localisation is that foreign governments may not have adequate data protection or privacy laws in place. If there are no adequate data protection laws in countries where data centres are located, there is a threat to privacy rights. The same concerns apply in instances where data are intended to be shared with a foreign government that does not have adequate privacy laws. One of the reasons why the ECJ ruled against Facebook and in favour of Mr Schrems[88] was because the US did not have adequate safeguards in place to prevent the US government from accessing any amount of data from EU citizens.

Another advantage of adopting data localisation measures is that it disincentivises foreign government entities. When data are stored within the servers of a country, the surveilling foreign state may expend a lot of resources and time to

83 Kuner, Data nationalism and its discontents, Emory Law Journal Online, vol. 64, 2014–2015, p 2089 (2091).

84 Jong-Chen, Georgetown Journal of International Affairs, 2015, p 112 (114).

85 Flaig, Lopez-Gonzalez, Messent and Jouanjean, 19th Annual Conference on Global Economic Analysis, 2016, p 1 (5).

86 Brehmer, American University Law Review, 2018, p 927 (930).

87 Ibid.

88 Maximillian Schrems v Data Protection Commissioner Case C-362/14, (Schrems I); Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18, "Schrems II").

gain access to this data.[89] This would be different in instances where one of the surveilling state's service providers has control over the data or the data are hosted within its territory. However, some view data localisation as a means for states to exercise domestic surveillance over their citizens.[90] In instances where a state conducts domestic surveillance over its citizens, the privacy rights of citizens are infringed. Data localisation can negatively impact user privacy and enterprise security by creating greater government access to user data.[91] The ease of access to data by law enforcement may result in domestic surveillance of citizens.[92] When governments implement data localisation strategies for their own political agendas, there is need to assess if such self-serving interests protect privacy rights of citizens. Strict data localisation laws have also been considered to promote political repression in some governments. If information is under governmental control, the government can easily suppress dissenting political opinions and threaten individual rights such as the rights to privacy, data protection, anti-discrimination and freedom of expression and democratic values.[93] An open internet enhances liberty as political dissidents often rely on foreign speech platforms to disseminate information. Data localisation can erode this benefit by preventing dissidents from using foreign based services or shrinking the services available to citizens as businesses will be reticent to operate data centres in authoritarian countries with strong state censorship and surveillance laws.[94]

While the prevention of foreign surveillance has been found to be a justifiable reason to localise data, there are still concerns that this reason is not justifiable. It has been argued that forcing data localisation of personal information to prevent foreign surveillance is flawed as many of the recent legislative proposals pre-date the surveillance revelations of Edward Snowden.[95] Mishra argues that data localisation does not prevent foreign surveillance. When data are hosted on local servers, it does not mean they are under an impenetrable shield. Foreign governments

89 Selby, International Journal of Law and Information Technology, 2017, p 213 (228).

90 Surveillance and related phenomena such as data localisation requirements have a bearing on citizens' right to privacy and other digital rights. Mapping and analysis of privacy laws in Africa 2021 CIPESA 1 at 28. Available at https://cipesa.org/resources/ (accessed on 4 June 2022).

91 Brehmer, American University Law Review, 2018, p 927 (931).

92 A study has shown that some states use access to data under their jurisdiction for local surveillance on citizens, which also violates the rights to privacy and threaten the rule of law. Adeleke, Mandela Institute Policy Brief 09, 2021, p 1 (4).

93 Fraser, SCRIPTed: A Journal of Law, Technology and Society, 2016, p 359 (366).

94 Ibid.

95 Bauer, Lee-Makiyama, Van Der Marel and Verschelde, European Centre for International Political Economy Occasional Paper No 3/2014, 2014, p 1 (3).

can still deploy covert surveillance tools to access the data if necessary.[96] Foreign surveillance pre-dates the use of cloud technologies. Due to the internet infrastructure, data localisation does not stop foreign surveillance. Furthermore, information security is not a function of where data are physically stored or processed and threats to data are oftentimes domestic.[97] Fraser also argues that in practice, governments denounce foreign surveillance on behalf of their citizens while secretly sharing intercepted information with others.[98] Fraser submits that considering this, localisation is not an effective means of keeping data from foreign intelligence agencies.[99] McKenna also argues that data localisation will not protect data stored in another state if the foreign state enjoys jurisdiction over the cloud service provider.[100] For example, the US has authority to compel Microsoft to disclose cloud data regardless of where the data are hosted.

D Do Data Localisation Measures Address the Growing Spectre of Cybercrimes?

Ironically, data localisation measures aimed at making it easier for law enforcement officers to access cloud evidence can potentially result in an increase in cybercrimes. When data are locally hosted on limited number of data centres, it creates an enticing target for those seeking to unlawfully access the data.[101] There are concerns that data localisation minimises the efficacy of corporate privacy and security controls and expands the corporate network.[102] If information is centralised and concentrated within specific servers in a country, it is more vulnerable to cyberattacks and external surveillance.[103] Pooling and storing data in designated

96 Mishra, Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows, Vanderbilt Journal of Transnational Law, 2019, p 463.

97 Bauer, Lee-Makiyama, Van Der Marel and Verschelde, European Centre for International Political Economy Occasional Paper No 3/2014, 2014, p 3.

98 Fraser points out that though Germany has been outspoken about America's PRISM program, it has a bilateral agreement with America to share information. Fraser, SCRIPTed: A Journal of Law, Technology and Society, 2016, p 359 (365).

99 Fraser, SCRIPTed: A Journal of Law, Technology and Society, 2016, p 359 (365).

100 McKenna, Up in the cloud: Finding common ground in providing for law enforcement access to data held by cloud computing service providers (2016) 49 Vanderbilt Journal of Transnational Law, vol 49, at 1438.

101 Fraser, SCRIPTed: A Journal of Law, Technology and Society, 2016, p 359 (363).

102 Brehmer, American University Law Review, 2018, p 927 (931).

103 Mishra, Vanderbilt Journal of Transnational Law, 2019, p 463 (496).

physical sites may result in less cybersecurity for data[104] making data an easy target for hackers.[105]

The African continent has weak domestic cybersecurity infrastructure which also results in less privacy protection.[106] This is also reinforced by the absence of cybercrime and cybersecurity laws in many African countries as well as the absence of an overarching legal framework. The AU Malabo Convention[107] provides a framework for both data protection (including cross border data flows), cybercrime and cybersecurity. It is important to note that countries with weak cyber security protections are at the forefront in advocating for data localisation measures.[108] Some argue that domestic companies may not have the same or better technologies that leading global companies have due to fewer financial resources, less available expertise, less competitive need to draw customers or the presence of technological restrictions.[109] These arguments, it should be noted, seem generalised and based on the assumption that local companies have less cybersecurity tools in place. To avoid such general assumptions, there is need for a detailed investigation of the implications of data nationalism[110] in the form of data localisation. Kuner takes issue with these arguments. He argues that hackers and national intelligence services tend to target large global data centres because they have more data to access, thus putting them more at risk.[111] It should be noted however that though bigger organisations may be attractive targets for syndicate cybercriminals, small businesses can still be seriously impacted by cyberattacks and cybercrime. With the prevalence of use of the internet and IoTs, different groups of cybercriminals have emerged, from inexperienced script kiddies who may target smaller businesses and individuals to criminal syndicates with experienced cybercriminals targeting big organisations and critical information infrastructure.

Successful cybercrime prosecutions are dependent on the investigating state being able to lawfully access electronic evidence either unilaterally or through the assistance of service providers. Adeleke argued that justifications for data localisation such as law enforcement purposes are not necessary in practice since

104 Sheppard, Yayboke and Ramos, Center for Strategic & International Studies, 2021, p 1 (7).
105 Shah, Yale Law Review Journal, 2015, p 543 (549).
106 Kugler, Mandela Institute Policy Brief 08, 2021, p 1 (7).
107 African Union Convention on Cyber Security and Data Protection 2014. Adopted by the 23rd ordinary session of the assembly held in Malabo, Equatorial Guinea on 27 June 2014 (the Malabo Convention).
108 Van der Berg, Mandela Institute Policy Brief 02, 2021, p 1 (6).
109 Fraser, SCRIPTed: A Journal of Law, Technology and Society, 2016, p 359 (363).
110 Kuner, Emory Law Journal Online, 2014–2015, p 2089 (2098).
111 Kuner, Emory Law Journal Online, 2014–2015, p 2089 (2096).

companies are mandated to comply with government access requests for data regardless of where the data may be stored.[112] This may not always be the case as service providers often deny access if data are stored in another country. As noted above, data localisation is likely to reduce the number of global service providers in a domestic market. Generally, local service providers do not have the financial resources and expertise compared to multinationals like Microsoft and Amazon.[113] This would potentially mean that the level of cooperation and assistance that may be offered to law enforcement agencies will be reasonably poor and limited. If domestic companies do not have better technologies or expertise to assist law enforcement agencies, that could potentially result in a decline in successful cybercrime prosecutions.

It should also be noted that the data localisation requirements set out in South Africa as well as in other African countries are new and yet to be fully implemented. As such, it is not possible to discern the exact extent to which these data localisation measures will assist law enforcement agencies[114] when accessing remote cloud data. Whilst there are economic benefits in unrestricted data flows, it is important to assess the benefits of data localisation vis-à-vis the storage and processing of data outside a country. This requires empirical research and empirical evidence, and both have yet to take place.[115] An analytical and empirical research on data localisation and its barriers should cover not only the scope and impact, but also the root causes and the design of governance mechanisms that could mitigate their negative effects.[116] Some have also argued that instead of providing law enforcement agencies with ease of access to electronic evidence, data localisation measures inhibit cybercrime investigations. It is argued that strict data localisation measures can further complicate an already convoluted and outdated MLAT system and increase barriers to law enforcement. Data localisation can potentially weaken current information sharing channels and businesses' reporting obligations, and ultimately impact intelligence gathering methods and criminal investigations.[117]

112 Adeleke, Mandela Institute Policy Brief 09, 2021, p 1 (4).
113 Fraser, SCRIPTed: A Journal of Law, Technology and Society, 2016, p 359 (363).
114 Beyleveld, Mandela Institute Policy Brief, 2021, p 1 (4).
115 Beyleveld, Mandela Institute Policy Brief, 2021, p 1 (7).
116 Drake, World Economic Forum, p 1 (5).
117 Sheppard, Yayboke and Ramos, Center for Strategic & International Studies, 2021, p 1 (7).

E Recommendations

I Adopt conditional instead of strict data localisation

Conditional or liberal data localisation requirements have the potential to strike the right balance between the interests of states to access evidence for crime investigation, the economic interests of businesses to share data globally and the individuals' privacy rights. Conditional data localisation measures promote the flow of data with limited restrictions while also ensuring the protection of privacy and personal data. Strict data localisation measures should be avoided and policymakers need to address the underlying challenges with existing legal mechanisms to improve the process of making cross-border requests for data.[118]

Strict data localisation measures prohibit both personal and non-personal data flows which may present a practical challenge for the success of the African free trade area and the envisioned African Digital Single Market as set out in the AU Continental Free Trade Agreement[119]. Instead of adopting strict data localisation measures, states should opt for conditional data transfers or sectoral data restrictions. The recently adopted AU Data Policy Framework can guide AU Member States on how to categorise data and share data while maintaining each State's sovereign interests. The AU Data Policy Framework acknowledges the importance of sovereignty of states over data but cautions against blanket data localisation and recommends collaboration and information sharing among Member States to improve data security.[120]

II Promote continental cooperation in criminal matters

The challenges of access to electronic evidence for criminal investigations cannot be effectively solved by data localisation measures. African States should not justify data localisation under the pretext of interests of law enforcement. The challenges presented by features of cloud data should be resolved, not by insisting on data localisation measures, but rather by promoting cooperation between states in criminal investigations. African countries need to build on existing bilateral and multilateral forms of cooperation and introduce new tools and mechanisms for co-

118 Cory and Dascoli, Information Technology and Innovation Foundation, 2021, p 1 (9).
119 African Union Continental Free Trade Agreement.
120 AU Data Policy Framework, p53.

operation. The coming into operation of the African Union Convention on Cyber Security and Personal Data Protection[121] (the Malabo Convention) can improve co-operation among African States in cybercrime investigations.

Article 28 of the Malabo Convention provides three ways in which AU Member States can foster cooperation and exchange information for law enforcement purposes. First, information can be exchanged between State Parties if there are mutual legal assistance agreements and State Parties are encouraged to conclude such agreements. AU Member States should build up on the existing agreements and conclude new agreements under the flagship of the Malabo Convention. Secondly, State Parties are encouraged to establish institutions that exchange information on cyber threats and vulnerability. This would include having more dedicated cybersecurity task forces like national computer emergency response teams (CERTs) and computer incident response teams (CSIRTs) working together with the AU Cybersecurity Expert Group. Thirdly, State Parties are encouraged to cooperate with international actors to respond to cyber threats, improve cybersecurity and stimulate dialogue between stakeholders. This includes collaborating with regional and international key stakeholders to review and identify national frameworks and practices related to cross-border data access.[122]

African countries should start negotiating bilateral and multilateral mutual legal assistance agreements in line with the Malabo Convention. Similarly, regional economic communities like SADC, EAC and ECOWAS should also develop and align their mutual legal assistance agreements with the Malabo Convention. Such agreements should be supported by an AU Cyber Security Strategy and a clear plan of action on the implementation of the Convention at national level. African countries without cybercrime laws and data protection laws can be supported by the AU if there is a guidance framework and implementation plan on how to domesticate the Malabo Convention. Part of the cooperation should extend to continent-wide capacity building programs designed and deployed to guide law enforcement agencies from AU Member States on issues around data protection and cybersecurity.

121 African Union Convention on Cyber Security and Personal Data Protection

122 Halefom, in: KM Yilma, The Internet and Policy Responses in Ethiopia: New Beginnings and Uncertainties, 2020, p 1 (42).

III Participate in global cooperation in criminal matters

Most African countries do not have jurisdictional leverage or means to compel foreign based service providers to enforce their laws in an extraterritorial manner[123] making data localisation measures futile. African States must cooperate at a global stage through notable and comprehensive frameworks on cooperation in criminal matters such as the Council of Europe Convention on Cybercrime[124] (the Budapest Convention). Signatories to the Budapest Convention have the advantage of assisting each other in criminal investigations in a more expedited manner. Parties to the Budapest Convention have addressed the complexity of obtaining electronic evidence in foreign and unknown jurisdictions by adopting the 2nd Additional Protocol to the Budapest Convention.[125] This protocol provides innovative tools for enhanced cooperation among Member States and permits State Parties to cooperate directly with service providers.

A small number of African countries are either parties to the Budapest Convention (Cabo Verde, Ghana, Mauritius, Morocco, Nigeria, and Senegal) or they have an observer status (Benin, Burkina Faso, Cameroon, Cote d'Ivoire, Niger, Rwanda, Sao Tome and Principle, Sierra Leone, South Africa and Tunisia).[126] Cabo Verde, Ghana and Mauritius recently signed the 2nd Additional Protocol.[127] African countries benefit more from being State Parties to the Budapest Convention as they are able to directly request for domain name registration information from registrars of other State Parties, directly cooperate with service providers in other State Parties to obtain subscriber information, get expedited support such as through video conferencing and in emergency situations. African countries should consider signing and ratifying the Budapest Convention and the 2nd Additional Protocol to get support on cybercrime investigations while also being actively involved in negotiating the United Nations treaty[128] on international cooperation on cybercrime.

123 Halefom, in: KM Yilma, The Internet and Policy Responses in Ethiopia: New Beginnings and Uncertainties, 2020, p 1 (30–34).

124 Convention on Cybercrime (ETS No. 185).

125 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

126 https://www.coe.int/en/web/cybercrime/parties-observers.

127 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224.

128 United Nations Resolution 75/282 on Countering the use of information and communications technologies for criminal purposes.

IV Develop and implement a clear cross border data transfer mechanism

The AU Data Policy Framework is the most recent step taken by African governments to consolidate the data environment and harmonise rules on data governance. The framework serves as a blueprint which provides an option for a common, coordinated and cohesive approach to data governance with guidance on data control, data processing, data protection, data access, data security, cross border data flows and creating the demand for data. The framework discusses aspects of data localisation within the context of law enforcement and makes a compelling case against data localisation. It points out that the security of data does not depend on the physical location of the servers hosting such data.[129] It also points out that some states are wrong in believing that data is more secure if it is stored within national borders. The framework points out that a cost-benefit assessment of localisation needs to be conducted against potential harm to human rights and broader economic development priorities. This framing can help African countries to move away from insisting on local storage of data to promoting the free and secure flow of data across the continent while safeguarding human rights, upholding security and ensuring equitable access and sharing of benefits.

F Conclusion

Data localisation enables law enforcement agencies to unilaterally and quickly access electronic evidence from local service providers without going through the long winding processes associated with MLAT channels. While African countries find it easier to assert digital sovereignty through data localisation mechanisms, such mechanisms should be avoided. Instead of insisting on local storage of data for purposes of law enforcement, African countries must find better solutions to address the underlying challenges of limited jurisdictional claims over foreign-based service providers and slow processes of MLAT channels. Such solutions include adopting conditional or sector specific data localisation requirements instead of a blanket ban to data transfer. With conditional data localisation, data will continue to be shared transborder subject to clear safeguards and guidelines to prevent abuse of personal data.

African countries should also improve and enhance cooperation in criminal matters by addressing the underlying challenges associated with traditional mutu-

129 AU Data Policy Framework p53.

al legal assistance. This includes finding innovative ways of fostering cooperation and expediting processes and engaging with service providers and domain name registrars. The Budapest Convention is a good example of a channel which can assist a lot of African countries to get expedited assistance in criminal matters especially where they do not have jurisdiction over foreign based service providers. Continentally, African States must adopt the Malabo Convention at national level and ensure that cybercrime, cybersecurity and personal data protection laws are adopted, implemented and enforced. This should be followed by negotiating mutual assistance agreements in line with the Malabo Convention. There is a general consensus at the AU level that data localisation measures have limited benefits for Africa. Through the AU Data Policy Framework, African countries can negotiate a cross-border mechanism which can be used to guide them when negotiating mutual assistance agreements.

G Bibliography

Adeleke, Exploring policy trade-offs for data localisation in South Africa, Kenya and Nigeria, Mandela Institute Policy Brief 09, 2021.

Bailey and Parsheera, Data localisation in India: Questioning the means and ends, National Institute of Public Finance and Policy, 2018.

Bauer, Lee-Makiyama, Van Der Marel and Verschelde, The costs of data localisation: Friendly fire on economic recovery, European Centre for International Political Economy Occasional Paper No. 3, 2014.

Beyleveld, Data localisation in Kenya, Nigeria and South Africa: Regulatory frameworks, economic implications and foreign direct investment, Mandela Institute Policy Brief 01, 2021.

Brehmer, Data localization: The unintended consequences of privacy litigation, American University Law Review, 2018.

Celestine, Cloudy skies, bright futures: In defense of a private regulatory scheme for policing cloud computing, University of Illinois Journal of Law, Technology & Policy, 2013.

Cory and Dascoli, How barriers to cross-border data flows are spreading globally, what they cost, and how to address them, Information Technology and Innovation Foundation, 2021.

Dalton, Van Vuuren, Jansen and Westcott, Building cybersecurity resilience in Africa, 12th International Conference on Cyber Warfare and Security, 2017.

Daskal, Privacy and security across borders, Yale Law Journal Forum, 2018–2019.

Daskal, Access to data across borders: The critical role for Congress to play now, Advance: The Journal of the ACS Issue Briefs, 2017.

Daskal, Borders and Bits, Vanderbilt Law Review, 2018.

Flaig, Lopez-Gonzalez, Messent and Jouanjean, Modelling data localisation measures, 19th Annual Conference on Global Economic Analysis, 2016.

Fraser, Data localisation and the balkanisation of the internet, SCRIPTed: A Journal of Law, Technology and Society, 2016.

Goldsmith, Sovereign difference and sovereign deference on the internet, Yale Law Journal Forum, 2018–2019.

Halefom, Government access to digital evidence across borders: Some lessons for Africa, in: KM Yilma (ed), The Internet and Policy Responses in Ethiopia: New Beginnings and Uncertainties, Addis Ababa University Press, 2020.
Hon, Millard and Walden, The problem of 'personal data' in cloud computing: what information is regulated? – the cloud of unknowing, International Data Privacy Law, 2011.
Jong-Chen, Data sovereignty, cybersecurity, and challenges for globalization, Georgetown Journal of International Affairs, 2015.
Koops and Goodwin, Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law, Tilburg Law School Research Paper Series, 2014.
Kugler, The impact of data localisation laws on trade in Africa, Mandela Institute Policy Brief 08, 2021.
Kuner, Data nationalism and its discontents, Emory Law Journal Online, vol. 64, 2014–2015.
Mishra, Building Bridges: International Trade Law, Internet Governance, and the Regulation of Data Flows, Vanderbilt Journal of Transnational Law, 2019.
Razzano, Data localisation in South Africa: Missteps in the valuing of data, Mandela Institute Policy Brief 06, 2021.
Resha, Addressing the potential for African digital governance to facilitate inclusive development: rights, rules & revenues, Discussion Paper, 2021.
Selby, Data localisation laws: Trade barriers or legitimate responses to cybersecurity risks, or both, International Journal of Law and Information Technology, 2017.
Sheppard, Yayboke and Ramos, The real national security concerns over data localization, Center for Strategic & International Studies, 2021.
Dan Jerker B Svantesson, Internet & Jurisdiction Global Status Report 2019, Internet & Jurisdiction Policy Network, 2019.
Tsosie, Tribal data governance and informational privacy: Constructing indigenous data sovereignty, Montana Law Review, 2019.
Van der Berg, Data protection in South Africa: The potential impact of data localisation on South Africa's project of sustainable development, Mandela Institute Policy Brief 02, 2021.
Woods, Litigating data sovereignty, Yale Law Journal, 2018.
Woods, Against Data Exceptionalism, Stanford Law Review, 2016.
Wu, Sovereignty and data localization, The Cyber Project Harvard Kennedy School, 2021.
Zheng, Comparative study on the legal regulation of a cross border flow of personal data and its inspiration to China, Frontiers of Law in China, 2020.
Hofmann, Towards an African narrative on digital sovereignty, 2022, https://www.hiig.de/en/publication/towards-an-african-narrative-on-digital-sovereignty/ (accessed 11 May 2023).
Digital Council Africa, Africa Digital Infrastructure Market Analysis 2021 Report, https://www.wcoesarpsg.org/wp-content/uploads/2021/11/juanita-clark-africas-evolving-digital-landscape.pdf (accessed 11 May 2023).

Legal instruments

African Charter of Human and Peoples Rights (ACHPR)
African Union Declaration of Principles on Freedom of Expression and Access to Information
African Union Convention on Cyber Security and Personal Data Protection 2014
African Union Data Policy Framework 2022

African Union Continental Free Trade Agreement 2018
Council of Europe Convention on Cybercrime 2001
Council of Europe Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).
European Union General Data Protection Regulation 2018
Nigeria Guidelines for Content Development in Information and Communication Technology 2013
Nigerian Data Protection Regulation (NDPR) 2019.
Nigerian Data Protection Bill, 2021.
South Africa Protection of Personal Information Act 4 of 2013.
South Africa Draft National Data and Cloud Policy 2021
United Nations Resolution 75/282 on Countering the use of information and communications technologies for criminal purposes
United Nations High Commissioner for Human Rights, The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights, Human Rights Council Thirty-ninth session, A/HRC/39/29
Zambia Data Protection Act 3 of 2021.

Part IV **Re-Imagining the Future**

Brian Tshuma

Data Imaginaries and the Emergence of Data Institutions in sub-Saharan Africa

A Introduction

The diversity and complexity of the African datasphere makes the continent's focus on data regulation on privacy, cybersecurity and data protection a subject of profound curiosity. Emerging concepts like 'data worlds,' 'data frontiers' or 'data futures' challenge conventional narratives about data, prompting a re-evaluation of data's potential by different data communities. The concepts are a way of looking beyond dominant narratives, as is canvassed in this chapter. A trendy way in which datafication is being reimagined today, and a foundation on which arguments in this chapter are based, is rethinking data as a public good that belongs to the people. This trend entails the creation of new, collective governance models and an alternative set of concepts and values to steer the new envisioned governance. Scholars and organisations across data traditions have highlighted data's varied impacts, advocating for new conceptual frameworks and values to guide enhanced data regulation. Focussing on sub-Saharan Africa, this chapter seeks to spotlight emerging data paradigms and explore novel insights into datafication. It points to the existence of alternative worldviews and new ways of thinking about data that inspire a novel set of institutional arrangements different from those popularised by the West.

Note: This chapter is an excerpt from an ODI Fellowship research paper.

https://doi.org/10.1515/9783110797909-012

B Rethinking Data

The idea of data imaginaries, a subfield of social imaginaries[1] inextricably linked to practice and action, challenges the global south to rethink the wholesale adoption of Western frameworks for structuring relations between technology and people. According to Beer, "data imaginar[ies] can be understood to be part of how people imagine data and its existence, as well as how it is imagined to fit with norms, expectations, social processes, transformations and ordering."[2] As new data imaginaries continue to sprout into different directions across the world, complementing, rivalling, or contesting the mainstream Big Data narrative,[3] African intellectuals, policy makers and other actors need to stretch their imagination beyond digital rights or the GDPR-type regulatory authorities in thinking about data and its governance. Davies (2022) has noted that data governance "has moved from being a niche topic … to becoming the overarching container for thinking about both data protection and access to data."[4] Data governance "has emerged as a key framework within which to address both the opportunities and the risks of data collection, sharing and use,"[5] in its various sphere of application (data communities). As such, the frameworks we rely on for data governance need to reflect this all-encompassing outlook in their approach.

Our imaginations do benefit from emerging conceptual frameworks, such as the datasphere, or data as public infrastructure, for example. The Datasphere can be understood as a data ecosystem, "the complex system encompassing all types of data and their dynamic interactions with human groups and norms."[6] Such a conceptual shift would 'bring into focus the interaction of datasets, norms and human groups,' and a move away 'from discussing relatively flat notions of "data governance"' built around privacy and protection. An all-inclusive framework offers an opportunity to account for the agency of different data communities who constitute Africa's datasphere (that is, data ecosystem). It will also

1 Taylor, Modern social imaginaries, *Duke University Press* 2004. Cf. Hintz et al, Civic Participation in the Datafied Society: Towards Democratic Auditing, *Data Justice Lab*, 2022.

2 Beer, Envisioning the Power of Data Analytics: The Data Imaginary – The Data Gaze: Capitalism, Power and Perception, *SAGE publications*, p. 5.

3 Citizen data imaginaries, *Data Justice Lab*, 2022.

4 Davies, Data Governance and the Datasphere: Literature Review, *Datasphere Initiative,* 2022 pp. 3 and 15.

5 Ibid.

6 de La Chapelle/Porciuncula, Hello Datasphere – Towards a Systems Approach to Data Governance, *Datasphere Initiative,* https://medium.com/@thedatasphere/hello-datasphere-towards-a-systems-approach-to-data-governance-d602f96c9e1d (accessed on 13.09.2023).

Fig. 1: Data communities who make up the datasphere (data ecosystem) in Africa.

facilitate new questions about responsibilities of data communities to be heard, *"and the interplay of norms, rather than simply the regulation of data through policy and law."*[7]

A data ecosystem encompasses multiple data communities spanning across public, private or civil society actors. It involves different types of data, personal or non-personal, individual or collective, with new and old institutions, norms, laws and policy frameworks, technologies, platforms or tools. The actors are involved in complex dynamic interactions with each other within the system. Regulatory responses, like Africa's preferred choice, which uses the GDPR as a one size fits all-regime for data governance, are simply inadequate. This is particularly so as more and more aspects of our everyday lives, 'play,[8] consumption,[9] work,[10] travel,[11]

7 Ibid.

8 For example, the Chinese App, TikTok connect people of similar interests and geographical proximity who socialise on the App.

9 Such asyoung people in Ghana livestreamed world cup matches on their smart phones using Apps while commuting from one suburb to another.

communications[12], domestic tasks,[13] security'[14] are 'being mediated, augmented, produced and regulated by digital devices and networked systems powered by [data systems]'[15]. In whatever domain these data innovations are deployed, they appear to be having a disruptive and transformative effect, both to how that domain is organised and operates and to the governance of opportunities, risks or challenges associated with them. There is no basis for Africa to confine its imagination to a one-sided GDPR discourse on data governance around privacy, digital rights, protection or control, when data continue to "adjudicate more and more consequential decisions in our lives."[16] There is a need to think beyond the GDPR framework, as has been done in the EU (the birth place of the GDPR), where additional frameworks have been (and continue to be) enacted (that is, the Data Act, the Digital Services Act, for example) to maximise social benefits of data beyond protection of privacy goals.

10 Taking an example ofEasyData, which publish South African economic data, including financial, trade, microeconomic and macroeconomic data. These infomediaries combine data from official statistics with data from various other sources.

11 An example is Google Live Traffic Alerts, Google began providing in April 2016 live traffic alerts in Kenya through its Google Maps mobile app when it is set to navigation mode. The app provides updated information on whether congestion is expected, and how long drivers may be stuck in traffic using a particular route. It then suggests alternative routes, including explanations of their advantages. The service is based on crowdsourced map data and traffic information from its active users.

12 For example, Budgit in Nigeria uses an array of tools to simplify the budget and matters of public finance for the people of Nigeria in order to enhance transparency, accountability and participation in public finance. It has developed a tool, Tracka, which allows Nigerians in 17 States to post pictures of development projects in their communities. Budgit's project officers aid citizens without Internet access to communicate with their elected representatives.

13 There is the rise of the 'Do It Yourself Movement' with most people downloading menus or instruction manuals from online platforms to their smart gadgets to complete tasks at home.

14 Apps on smart phones.

15 Civil society actors such as Map Kibera in Kenya and Ramani Tandale in the United Republic of Tanzania are specifically focused on open data and often integrate geospatial, crowdsourced and official data of relevance to particular communities, regions and peoples. Also, private-sector firms, especially technology companies, are engaging with national data ecosystems by facilitating platforms for crowdsourced or citizen-generated data, Ushahidi for example.

16 Diakopolous, Algorithmic Accountability: On the Investigation of Black Boxes, *Columbia Journalism Review: Tow Report*, December 2014, available at: https://www.cjr.org/tow_center_reports/algorithmic_accountability_on_the_investigation_of_black_boxes.php (accessed on 13.09.2023).

C The Big Data Imaginary

The prevalent market imaginary (that is, the Big Data narrative) 'foregrounds human agency as individual market choice, where personal data serves the interests of individuals.'[17] It undergirds the function of digital technologies in rendering data into algorithmic knowledge, often subversive of traditional value systems such as *Ubuntu,*[18] *Umoja,*[19] *Kujichagulia,*[20] *Ujima,*[21] *Nia,*[22] *Kuumba,*[23] *or Imani,*[24] popular among peoples of Africa for example. Heavily promoted by the liberal West and an array of associated epistemic centres, the Big Data imaginary is based on a quantitative ontology which stresses the mathematical and computational properties of algorithms. Seaver laments this as having the effect of ensuring that "[o]ther knowledge about algorithms – such as their applications, effects, and circulation – is strictly out of frame."[25] It tends toward homogenisation and standardization of data within categories. Tironi and Barragán's study of data-driven initiatives examined impacts of hyped expectations and promises in Chile, underscoring the importance of not taking as given any sort of homogeneous or universal 'datafication' process and problematize how data-driven and smart governance are enacted – not without problems and breakdowns in each location. Its foundations in objectivity abstracts governance to notions beyond understanding by ordinary citizens.[26] Silvia Masiero and Soumyo Das' studies of India's Adhaar's program call for a move towards ways in which data is integrated into systems of

17 Hintz et al., Civic Participation in the Datafied Society: Towards Democratic Auditing?: A Research Report *Data Justice Lab*, 2022, available at: https://datajusticelab.org/wp-content/uploads/2022/08/CivicParticipation_DataJusticeLab_Report2022.pdf (accessed on 13.0.2023).

18 Humanity – to endeavour to make practical mutual humanity as a basis of human society.

19 Unity – to strive for and to maintain unity in the family, community, nation, and race.

20 Self-determination – to define ourselves, name ourselves, create for ourselves, and speak for ourselves.

21 Collective work and responsibility – to build and maintain together and our brothers and sisters' problems our problems and to solve them together.

22 Purpose – to make our collective vocation the building and developing of our community in order to restore our people to their traditional greatness.

23 Creativity – to do everything we can to leave our community more beautiful and beneficial than we found it.

24 Faith -to believe with all our heart in our people, our parents, our teachers, our leaders and the righteousness and victory of our struggle.

25 Seaver, Knowing algorithms. Paper presented at Media in Transition 8, Cambridge, MA., i2013) https://digitalsts.net/wp-content/uploads/2019/03/26_Knowing-Algorithms.pdf accessed on 13.09.2023.

26 Tironi/Barragán, Designing the city by numbers? Introduction: Hope for the Data-Driven City, (2018) *Datactive* https://data-activism.net/2018/04/blog-designing-the-city-by-numbers-bottom-up-initiatives-for-data-driven-urbanism-in-santiago-de-chile/.

governance, and discuss its social justice implications. Finally, it operates by simplifying and taking the data out of its original contexts.[27] Ulises and Couldry advise that attention should be directed at how data infrastructures "alter the way people make sense of themselves and of the world around them," or how interpersonal connections and interactions are datafied through processes around these infrastructures.[28] As such, algorithmic devices cannot be divorced from the conditions under which they are developed and deployed.[29] This is in no way an attempt to undermine the GDPR regime of data protection, the intention is to expose its acclaimed universality, moral neutrality or computational rationality as mere rhetoric that it is.[30]

D Alternative Imaginaries

A fashionable way in which datafication is being reimagined today, and the point I make in this chapter, is rethinking data as a public good that belongs to the people. Rethinking data as public infrastructure entails the creation of fresh, collective governance models and an alternative set of concepts and values to steer a fast-evolving ecosystem, that is, the datasphere. Data as a public good requires sharing of data across sectors and ending data fragmentation, data hoarding or building of data silos common under the GDPR regime. The African Open Data Report has noted that, 'open data can be used to create social, economic and business value by facilitating better governance, public services and decision-making, supporting new businesses and improving the climate for foreign investment.'[31] The challenge remains how to make these often proprietary[32] data available for social or public

27 Masiero/Das, Datafying Anti-Poverty Programmes: Implications for Data Justice, *Information, Communication & Society*, 22 2019, 916.

28 Ulises/Couldry, Datafication, *Internet Policy Review* 8, 2019, available at: https://policyreview.info/concepts/datafication (accessed on 13.09.2023).

29 Geiger, Bots, Bespoke, Code and the Materiality of Software Platforms, *Information, Communication & Society*, 17 2014, 342.

30 Laws (legislation) or governance is by nature context based phenomena which bares the ontological, axiological or epistemological imprints of its crafters and the people involved. These are subject matters. Without undermining the GDPR, the argument is, presenting it (GDPR) as universal, apolitical or objective is misleading.

31 African Development Bank, Economic Benefits of Open Data in Africa, Report of March 2017.

32 The word "proprietary" is used in its ordinary English language dictionary meaning, to refer to 'relating to an owner or ownership.' In this regard, the professed relation between data and big corporations like Alibaba, Meta, Tencent, Google, Apple, Baidu, or Sensetime.

purposes in ways that do not diminish their commercial viability for their producers.

A variety of models for striking the balance in making data available for public innovations without compromising its proprietary value are currently being piloted in Africa. Examples of such models and bottom up data institutions are data pools, data commons, data exchanges, data unions or data trusts and Open Algorithm Project,[33] the Lacuna Fund[34] or Abalobi[35]. The role of data institutions is to collect, maintain and share data.[36] Specific responsibilities would include independent gate keeping, developing standards and identifiers, publishing open data, facilitating safe access, empowering people or generating insights.[37] New concepts include looking at data as a public good or data as public infrastructure, a good example of which is the Google Live Traffic Alerts project in Kenya.[38] The proliferation of technologies such as Ushahidi (in Kenya),[39] GhanaPostGPS (in Ghana)[40], What3words (in Ivory Coast)[41] or Ecocash (in Zimbabwe)[42] in sub-Saharan Africa

33 A pilot platform for unleashing the power of big data held by private companies for the public or social good in a privacy-preserving, commercially sensible, stable, scalable, and sustainable manner. It consists of an open technology platform and open algorithms running directly on the servers of partner companies, behind their firewalls, to extract key development indicators of relevance for a wide range of potential users, including national statistical offices, ministries, civil society organizations and media organizations. It is currently being piloted in selected African, Asian and Latin American countries.

34 Lacuna Fund is a collaborative effort to provide data scientists, researchers and social entrepreneurs in low- and middle-income context with the resources they need to produce labelled datasets that address urgent problems in their communities.

35 Abalobi is a South African-based, global social enterprise. Its to contribute towards thriving, equitable, climate change resilient and sustainable small-scale fishing communities globally, through the joint development of Technology for Good.

36 Available at https://theodi.org/article/the-data-institutions-register/.

37 Available at https://www.theodi.org/event/sharing-data-better-the-rise-of-data-institutions/.

38 Ibid.

39 Ushahidi is an open-source software application which utilises user-generated reports to collate and map data. It uses the concept of crowdsourcing serving as an initial model for what has been coined as "activist mapping" – the combination of social activism, citizen journalism and geographic information.

40 The GhanaPostGPS is a phone-based application which is designed to locate physical features anywhere in Ghana. It is Ghana and the sub-Saharan Africa's only official digital property addressing system which covers every inch of the country, ensuring that every location has a digital address.

41 What3words is a digital address app, an easy-to-remember system for identifying any 3-meter square in the world, good for commerce and navigation in the African nation.

42 Ecocash is a data based mobile financial services platform in Zimbabwe with a range of functionalities including credit vetting on the basis of social scoring criteria.

speaks to the importance of data-sharing and integration. It also points to the importance of models for making data within a single data community available to broader groups in other data communities in the African datasphere. While the idea of data as a valuable resource is clear in private companies and has led to useful innovations, this concept is not well developed in Africa. Boyera and Iglesias have expressed concern about the lack of knowledge about "the relationship between socioeconomic and political contexts, open licences, technical platforms and the dynamics of data use and outcomes (intended and non-intended) in different countries or sectors."[43] They also lamented the involvement of a few actors in the community and further that "there is still underinvestment in the sector in terms of both donor and State funding."[44]

E Conclusion

The idea that Big Data[45] is the only accepted way to understand the world is no longer valid. Africa needs to find new ways to connect people, information and knowledge that align with its values and heritage. The spirit of collectiveness seen in concepts like ubuntu suggests a different way of looking at data, where everyone has a role to play. Market based governance has limitations, and a more holistic approach could benefit the public. Just as in the West, where mechanisms like citizen assemblies, citizen councils or citizen summits are being adopted as governance tools for involving ordinary people in AI policy making, Africa can use its heritage to create a new set of data institutions that reflects its values[46].

43 Boyera/Iglesias, Open Data in Developing Countries: State of the Art, Partnership for Open Data – London, 2014.

44 Ibid. 43. Hintz et al, Civic Participation in the Datafied Society: Towards Democratic Auditing, *Data Justice Lab*, 2022.

45 The term "Big Data" is used as a way of thinking, an approach to collecting, managing, processing, interpreting, analysing, owning, using or reusing, as well as disposal of data associated with and popularised by Big Tech. Data as not possible of personal or group ownership, data as oil, data as a resource available out there for exploitation by anyone, data as a *'res nulius'*.

46 In the West, policy makers use analogues of unions, exchanges, trusts, common grazing pastures, or cooperatives to build data institutions for managing data in the public interests as opposed to the private interest. My argument is that Africa can and must look to similar innovations among its peoples instead of simply copy pasting Western analogies. A good example of an African analogy is what is called *'Igombana laBashe'* in Zimbabwe, a practice in terms of which households in a community contributed a portion of their grain harvest to a central repository managed by the King. This repository was not for the King's private use, the King held it on behalf of the community and any household who fell short of grain supplies could approach the King for temporal relief. This is a perfect

Ubuntu and similar belief systems can inspire new ways of thinking about data value creation. Africa should use these values to set up data institutions that match the moral fabric of its people. After all, '[t]he collective data imaginaries are the fuel from which more just datafied societies can emerge and thrive[!]'43

F Bibliography

African Development Bank, Economic Benefits of Open Data in Africa, Report of March 2017.

Beer, Envisioning the Power of Data Analytics: The Data Imaginary – The Data Gaze: Capitalism, Power and Perception, SAGE publications, p. 5 (2019).

Boyera/Iglesias. Open data in developing countries: State of the art. London: Partnership for Open Data (2014).

Citizen data imaginaries, Data Justice Lab (2022).

Davies, Data Governance and the Datasphere: Literature Review, *Datasphere Initiative 2022*.

de La Chapelle/Porciuncula, Hello Datasphere – Towards a Systems Approach to Data Governance, *Datasphere Initiative*, https://medium.com/@thedatasphere/hello-datasphere-towards-a-systems-approach-to-data-governance-d602f96c9e1d (accessed on 13. 09. 2023).

Diakopolous, Algorithmic Accountability: On the Investigation of Black Boxes, *Columbia Journalism Review: Tow Report* (2014), available at: https://www.cjr.org/tow_center_reports/algorithmic_accountability_on_the_investigation_of_black_boxes.php (accessed on 13. 09. 2023).

Geiger, Bots, Bespoke, Code and the Materiality of Software Platforms, *Information, Communication & Society* 17 (2014).

Hintz/Dencik/Redden/Treré/Brand/Warne, Civic Participation in the Datafied Society: Towards Democratic Auditing, Data Justice Lab, University of Cardiff (2022).

Masiero/Soumyo, Datafying Anti-Poverty Programmes: Implications for Data Justice, *Information, Communication & Society* 22 (2019).

Mejias/Ulises/Datafication, *Internet Policy Review* 8 (2019) https://policyreview.info/concepts/datafication (accessed on 13. 09. 2023).

Open Data in Developing Countries: State of the Art, Partnership for Open Data – London (2014).

Seaver, Knowing Algorithms, Paper presented at Media in Transition 8, Cambridge, MA. (2013), available at: https://digitalsts.net/wp-content/uploads/2019/03/26_Knowing-Algorithms.pdf (accessed on 13. 09. 2023).

Taylor, Modern social imaginaries, Durham: Duke University Press (2004).

Tironi/Barragán, Designing the city by numbers? Introduction: Hope for the Data-Driven City, *Datactive* (2018), available at: https://data-activism.net/2018/04/blog-designing-the-city-by-numbers-bottom-up-initiatives-for-data-driven-urbanism-in-santiago-de-chile/ (accessed on 13. 09. 2023).

Available at: https://theodi.org/article/the-data-institutions-register/ .

Available at: https://www.theodi.org/event/sharing-data-better-the-rise-of-data-institutions/.

analogy around which a bottom-up data institution can be developed. People contribute their data to a common repository, managed by some central authority for the benefit of the community. This, in my view is a better point of departure for African peoples than the analogies of Trusts, used for Data Trusts for examples.

Author Profiles

Dr. Patricia Boshe is a senior researcher at the Research Centre for Law and Digitalisation (FREDI) at the University of Passau, Germany.

Peter Kimpian is the Secretary to the Committee of Convention 108.

Dr. Lukman Abdulrauf is a 2022–23 Fellow at the Center for Advanced Study in the Behavioural Sciences, Stanford University, Department of Public Law, University of Ilorin, Nigeria, and Honorary Research Fellow, School of Law, University of Kwazulu-Natal, South Africa.

Prof. Mailyn Fidler is an Assistant Professor, University of New Hampshire Franklin Pierce School of Law and Faculty Affiliate, Berkman Klein Center for Internet & Society at Harvard University, U.S.A.

Dr. Iheanyi Samuel Nwankwo, is a post-doctoral researcher, currently works in the area of European Data Protection at the Institute for Legal Informatics, Leibniz Universität Hannover, Germany.

Nelson Otieno Okeyo, LL.M is a doctoral researcher in the field of business and human rights at Friedrich-Alexander-University of Erlangen-Nürnberg and a PhD student at the University of Bayreuth, Germany.

Setor Foe-Ahorney is a legla practitioner and consultant in Ghana. She is also a mentor for the Global Women Development Promoters (GLOWDEP), and currently pursuing an executive Master of Business Administration (EMBA Project – Management) at the University of Ghana Business School, Ghana.

Ridwan Oloyede is a co-founder of TechHive Advisory, where he leads the tech policy team.

Aishat Salami is an experienced legal practitioner and leads the technology policy and research team at Veeta Advisory Hub.

Victoria Oloni is an innovative lawyer with significant interest in Digital Economy, Data Protection, Cybersecurity and general intersections of Technology and Law.

Dr. Melody Musoni is a policy officer at the Centre for Africa-Europe Relations (ECDPM) in the digital economy and governance team.

Brian Tshuma is a capital markets lawyer in alternative investments -hedge funds, private equity, futures, options, or other securities, is a junior research fellow at the Open Data Institute, London.