African Journal on Privacy & Data Protection

2024

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

The financial support of Meta is gratefully acknowledged

African Journal on Privacy & Data Protection

Volume 1 ~ 2024

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

2024

African Journal on Privacy and Data Protection

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

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

Printed and bound by:
Pinetown Printers, South Africa

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

Cover design:
DN Ikpo

ISSN: 3007-8997

African Journal on Privacy & Data Protection

https://doi.org/10.29053/ajpdp.v1i1

Contents

African Journal on Privacy & Data Protection

Editorial ~ Volume 1, 2024

https://doi.org/10.29053/ajpdp.v1i1.0001

The *African Journal on Privacy and Data Protection* (the *Journal*) is domiciled in the Faculty of Law, University of Lagos Akoka-Lagos, Nigeria and published once a year by the Pretoria University Law Press (PULP) in South Africa. The *Journal* is peer reviewed and open access.

The main aims of the *Journal* are to promote African expertise and literature in the area of privacy and data protection. More specifically, the *Journal* aims to –

- foster African-centred research and knowledge generation on privacy and data protection;
- fill the critical knowledge gaps in this area as well as encourage privacy and data protection discourse from African perspectives;
- facilitate access of African scholars to new and developing knowledge in privacy and data protection as well as showcase African scholars and perspectives to the world; and
- become the leading academic journal on privacy and data protection on the continent and beyond.

Against this backdrop, this volume of the *Journal* publishes ten articles that further the objectives and mission of the *Journal* as the leading academic journal on privacy and data protection in Africa. The articles address issues relating to origin of privacy in Africa; cross-border transfers of data on the African continent; data protection and privacy in the context of social media influencing; data protection in the context of digital surveillance and big data; privacy and data protection issues in national social support programmes; the regulation of artificial intelligence through data protection laws, and so forth. The jurisdictional scope of the articles truly is African and diverse, featuring scholarship from South Africa, Malawi, Kenya, Zimbabwe, Nigeria, and so forth.

In the first article of the volume, Jimoh opened with a debate between Alex B Makulilo and Kinfe Yilma on the origin of privacy in Africa. Jimoh argues that contrary to Makulilo's submission that the concept of privacy was imported into Africa from the West, there is evidence that privacy existed in Africa before contact with the West. Thus, he agrees with Yilma who holds the view that privacy is innate to Africa, but he goes further than Yilma to provide ample evidence to solidify his claim of autochtony of African idea of privacy.

Next, Khaoma and Wanjiku make a case for continental cooperation in the harmonisation of a regional legal framework for cross-border data transfers in Africa. In this article they attribute cross-border data transfer to the need of the growing digital economy across Africa and the world. They note that the fragmented legal frameworks and approaches for cross-border data transfer on the continent lead to data localisation which is inadequate to address the need of growing digital economies. To forestall a situation that will will stymie the digital economy expansion on the continent, they recommend the formulation of a comprehensive continental legal framework that balances the imperatives of data protection and privacy with the boundless opportunities of unfettered digital economy.

This was followed by Mutiro and Saki who conduct a comprehensive critical review and analysis of the Cyber and Data Protection Act of Zimbabwe (CDPA). They note that while the CDPA is a significant statutory development over the Access to Information and Protection of Privacy Act (AIPPA) which it replaces, the focus of the CDPA is more on cyber security that it prioritises over the privacy of citizens. They identify major data protection weaknesses and gaps of the CDPA, to include the absence of an independent right to data protection in the Act; a failure to include important data subject rights such as the right to be forgotten, the right to access the courts for violation of the CDPA; the incapacity of the DPA to prescribe administrative sanctions; non-independence of the DPA, and so forth. The authors recommend the rectification of the gaps through regulations issued in terms of the CDPA or through guidance by the DPA (POTRAZ).

Goliath subsequently discusses the right to privacy of children social media influencers under the South African Protection of Personal Information Act 4 of 2013 (POPIA). She argues that as social media influencing has become more popular in Africa, children have begun to take part, often through their parents. She assesses the extent and effectiveness of the protection provided for children social media influencers by POPIA on three grounds: the scope of the protection provided by POPIA; the consent requirement when children's personal information is to be processed; and the available relief mechanisms. She concludes that the POPIA in its current formulation is defective on the three grounds and does not give adequate protection to children social media influencers or sufficiently engage the changing landscape of the digital age and social media influencing in relation to the rights of children to privacy.

On his part, Akintayo interrogated the trends and implications of Nigerian courts' jurisprudence on privacy and data protection. He highlights the importance and role of the judiciary in ensuring that the law keeps pace with the rapid development of technology. He notes that the preponderance of the cases decided by Nigerian courts on privacy and data protection tend to follow the traditional and narrow interpretation of the right to privacy that disavow connection between privacy and data protection. Drawing lessons from comparative foreign jurisprudence, he analyses the changing paradigm of privacy in comparative foreign jurisprudence in light of emerging technologies and identifies best practices and learning points for Nigerian courts.

Sato evaluates protection afforded the right to privacy and personal data processing under Malawi's national social support programmes. The author interrogates the extent to which data protection mechanisms are reflected in the Unified Beneficiary Registry (UBR), the framework through which the national social support programmes in Malawi are implemented. The author demonstrates that the mechanisms in place under the UBR are inadequate and recommends the adoption of a comprehensive data protection regime to address contemporary data protection problems under the UBR.

Two contributions in this volume seek to balance the states' cybersecurity and surveillance regimes with citizens' right to privacy. In his article, Salau observes that there is mutual dependence and nexus between cybersecurity and state surveillance that impacts the right to online privacy. After reviewing African and Nigerian cybersecurity and state surveillance frameworks, he concludes that there are several gaps in Nigeria's state surveillance frameworks in comparison to evolving international standards. Using the liberal democratic theory principles as theoretical underpinning to the article, he argues that a binary conception of privacy into a private/public dichotomy has become obsolete in the internet age. He made the case for law and policy reforms that privilege citizens' online privacy as well as promote the cherished democratic values of autonomy, accountability and transparency in Nigeria's cybersecurity and state surveillance regimes.

Khamala, writing on Kenya, interrogates the effects and impacts of mass surveillance through big data on the right to privacy in Kenya. He examines Kenyan courts' decisions on big data and finds that the courts initially adopted a broad privacy approach but later reverted to a narrow approach permissive of generalised surveillance and consequently, potential violation of the rights to privacy and dignity of citizens. He notes that in so far as Kenya's data protection framework is deficient in that it privileges national security over the right to privacy, it provides a poor basis for judicial oversight over generalised surveillance.

There are also two contributions that analyse the privacy and data protection dimension of artificial intelligence (AI) in South Africa and Nigeria, respectively. In their article, Davis and Trott undertake a review and analysis of the potentials of data protection laws to regulate AI on the African continent. They observe that

AI is poorly regulated on the continent and that the only form of regulation of AI in most African states comes in the form of data protection laws. Drawing insights from the South African data protection framework – the Protection of Personal Information Act 4 of 2013 (POPIA) – the authors argue that POPIA provides ineffective and inadequate regulation of AI as it fails to adequately engage with the unique attributes and operations of AI. The Act thus provides very limited protection for the rights of data subjects implicated by AI. They recommend that African states take meaningful steps through domestic legislation to urgently address the governance lacuna of AI on the continent.

Salami and Nwankwo in their article examine the extent to which Nigeria's data protection frameworks address concerns emanating from personal data processing in AI systems' life cycles, that is, from development to deployment. They observe that while there are data protection principles and requirements that can potentially be used to engage the concerns and challenges of data processing in the development and deployment of AI systems, the principles and requirements may not be adequate to fully and effectively tackle the concerns and challenges of AI systems. They recommend the development of a comprehensive AI human rights framework in alignment with global best practices and the harmonisation of Nigeria's data protection frameworks into a single framework, and so forth.

On the whole, all the contributions in this volume resonate with and advance the aims and objectives of the *Journal* in significant ways. The editorial board extends its profound gratitude to the scholars and experts who graciously peer reviewed articles in this volume in order to ensure the quality of the *Journal*. We look forward to working with you again in the future.

Dr Akinola Akintayo
Managing Editor
March 2024

African Journal on Privacy & Data Protection

To cite: M Jimoh 'The quest for information privacy in Africa: A critique of the Makulilo-Yilma debate ' (2024) 1 *African Journal on Privacy & Data Protection* 1-17
https://doi.org/10.29053/ajpdp.v1i1.0002

The quest for information privacy in Africa: A critique of the Makulilo-Yilma debate

*Mujib Jimoh**
Research Associate, Duke University School of Law

Abstract

In 2017 Kinfe M Yilma wrote a review in the Journal of Information Policy, which critiques Alex B Makulilo's two books – Privacy and data protection in Africa and African data privacy law. Yilma rejects, among others, Makulilo's conclusion that the African concept of privacy is more of an import from the West than an indigenous notion. Yilma states that privacy was present in Africa before contact with the West and that the omission of a privacy provision in the African Charter was a 'mere drafting oversight'. However, Yilma provides no proof that privacy existed in Africa before contact with the West. When Makulilo published a reply to this review in 2018, he capitalises on Yilma's lack of proof. In his reply, Makulilo reiterates the assertion in his two books by providing some evidence that, to him, proves that privacy indeed is a foreign concept imported to Africa. This article names this debate between these two leading scholars on privacy in Africa the 'Makulilo-Yilma debate'. The article is investigative. It interrogates this

* LLB; LLM (Duke Law School); mujib.jimoh@duke.edu; mujibjimoh@yahoo.com. 'The quest for information privacy in Africa' is an article by Alex B Makulilo, published in the *Journal of Information Policy* in response to Kinfe Michael Yilma's article titled 'The quest for information privacy in Africa: A review essay', also published in the *Journal of Information Policy*. Both articles, albeit not conforming, raise some critical arguments about privacy in Africa. This article seeks to interrogate the debate.

debate and underscores the fallacies contained in it. It will investigate the claims of both scholars. In doing so, it seeks to scrutinise the claim that the absence of a privacy provision in the African Charter was a 'mere drafting oversight'. Principally, providing legal, cultural, and sociological proofs, it will argue that privacy existed in Africa before contact with the West – an exercise lacking in Yilma's review – and a claim with which Makulilo, through his scholarship, has disagreed.

Key words: privacy; Africa; African Charter; Makulilo; Yilma

1 Introduction

One important aspect to be considered in the quest for information privacy in Africa is to understand the origin of privacy in Africa in order to ascertain how best to protect it in modern times.[1] Two African scholars who have attempted to locate this origin in the quest for information privacy in Africa are Alex B Makulilo and Kinfe M Yilma. In 2017 Yilma wrote a review of Makulilo's two books, *Privacy and data protection in Africa* and *African data privacy law*, in the *Journal of Information Policy*.[2] Essentially, Yilma rejects Makulilo's conclusion that the African concept of privacy is more of an import from the West than an indigenous notion. A year later, Makulilo responded to this critical review, also in the *Journal of Information Policy*,[3] reiterating his proposition that privacy indeed is a foreign concept imported to Africa. Both the review by Yilma and the reply by Makulilo exemplify a debate in the legal space. Typically, a debate involves two sides: one side in support of a proposition, and the other side opposing it. In Dworkin's thesis, there are bound to be disagreements in the legal space since law is argumentative in nature, where normative arguments are deployed.[4] This article tags both the review and reply the 'Makulilo-Yilma debate'.

In discussing this debate, the article argues that the right to privacy, like other human rights, has cultural dimensions,[5] and should be seen in that light. It posits that in the quest for information privacy in Africa in modern times, it is imperative to always bear in mind the culture, philosophy and the prevailing socio-economic structures of Africa. As Motala observed, 'no single document can represent a blueprint of the full content of "human rights"'. This is because the substance of 'human rights' depends on the cultural setting of a particular society. Moreover, specific human rights doctrines interrelate with prevailing socioeconomic

1 M Jimoh 'The place of digital surveillance under the African Charter on Human and Peoples' Rights and the African human rights system in the era of technology' (2023) 1 *African Journal of Legal Issues in Technology and Innovation* 113.
2 KM Yilma 'The quest for information privacy in Africa: A review essay' (2017) 7 *Journal of Information Policy* 111-119.
3 AB Makulilo 'The quest for information privacy in Africa' (2018) 8 *Journal of Information Policy* 317-337.
4 LR Ludeña 'Legal disagreements: A pluralist reply to Dworkin's challenge' (2016) 28 *Revus* 11.
5 M Mutua 'Savages, victims, and saviours: The metaphor of human rights' (2001) 42 *Harvard International Law Journal* 201-246.

structures.'[6] In part, the Makulilo-Yilma debate shares this reasoned notion,[7] yet, the debate commits some fallacies that this article seeks to address.

The article seeks to argue that within the communal ontology of the pre-colonial African societies, privacy existed. In doing so, the article rejects Makulilo's view that privacy was a Western concept. While it agrees with Yilma that privacy was not imported to Africa, it seeks to provide evidence of privacy in precolonial Africa, an exercise lacking in Yilma's scholarship. The article adopts the Neethling theory of privacy, where privacy is defined as

> an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself [or herself] at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he [or she] evidences a will for privacy.[8]

It discusses the importance of culture in the quest for information privacy in Africa. In its scope, it will limit its analysis to Yilma's critique of chapter 5 of Makulilo's *Privacy and data protection in Africa*[9] and Makulilo's response thereto.[10] The article will highlight the fallacies contained in the review and the reply. In undertaking this analysis, the article will be divided into five parts. After this introduction, part 2 will summarily discuss the main thesis of the Makulilo-Yilma debate. Part 3 will examine the fallacies in Yilma's review. Part 4 will discuss the fallacies in Makulilo's reply. The fifth part will outline the conclusion.

2 The Makulilo-Yilma debate

A critical appraisal of the Makulilo-Yilma debate reveals that the debate seems to be a sub-set of the 'African values and the human rights debate'[11] of the 1980s dominated by scholars such as Howard,[12] Donnelly,[13] Okere,[14] Cobbah[15] and Motala,[16] who all considered the place of culture and the societal philosophy on

6 Z Motala 'Human rights in Africa: A cultural, ideological, and legal examination' (1989) 12 *Hastings International and Comparative Law Review* 373.
7 See, eg, Makulilo (n 3) 321.
8 J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 18-28. Scholars such as Roos and Makulilo agree with this theory. See A Roos 'The law of data (privacy) protection: A comparative and theoretical study' unpublished PhD thesis, University of South of Africa, 2003 554; AB Makulilo 'A person is a person through other persons – A critical analysis of privacy and culture in Africa' (2016) 7 *Beijing Law Review* 196.
9 Yilma (n 2) 114-115.
10 Makulilo (n 3) 331.
11 J Cobbah 'African values and the human rights debate: An African perspective' (1987) 9 *Human Rights Quarterly* 309-331.
12 R Howard 'The full-belly thesis: Should economic rights take priority over civil and political rights? Evidence from sub-Saharan Africa' (1983) 5 *Human Rights Quarterly* 467-490.
13 J Donnelly 'Cultural relativism and universal human rights' (1984) 6 *Human Rights Quarterly* 400-419.
14 BO Okere 'The protection of human rights in Africa and the African Charter on Human and Peoples' Rights: A comparative analysis with the European and American systems' (1984) 6 *Human Rights Quarterly* 141-159.
15 Cobbah (n 11).
16 Motala (n 6).

human rights.[17] Yilma states in his review that 'the omission of a right to privacy provision in the Charter has been the source of *a rather illogical conclusion* about the absence of innate privacy demands in African societies'.[18] Yilma does not state the concluders. In this regard, Makulilo remarks that Yilma does not point out 'who is the accused person'.[19] However, I rather imagine that Yilma is referring to scholars such as Motala, Cobbah and Swanson[20] whose true view was that the conception of a right (whether privacy, or any other) depends on how it is conceptualised in that society.[21] Yilma must have misinterpreted these.

Yilma's review contains critical commentaries on Makulilo's *Privacy and data protection in Africa*[22] and *African data privacy law*.[23] On the critique of chapter 5 of *Privacy and data protection in Africa,* which is the focus of this article, Yilma accuses Makulilo of relying on ubuntu, a notion Yilma claims to be used mostly in Southern Africa, to generalise that privacy is more of an import from the West rather than an indigenous notion.[24] Yilma then states that 'readers might find this claim to be a generalisation about a rather heterogeneous continent of fifty-four nations with diverse ethnic and cultural backgrounds'.[25] In general, the main thesis of Yilma's review is that privacy was not an import from the West to Africa, although Yilma does not provide a cogent proof of this, other than stating that 'several African countries have had some form of privacy protections in their constitutions and civil laws long before the Banjul Charter was adopted'.[26] In part 3 this article discusses the reason why Yilma's assertion that the presence of privacy in these constitutions denotes innate privacy in traditional African societies is premised on a false ground. It will go further to provide some evidence Yilma ought to have provided.

Yilma takes the argument further, accusing Makulilo of 'briefly' considering the absence of an express privacy provision in the African Charter on Human and Peoples' Rights (African Charter)[27] and stating that the *omission* of privacy in the African Charter 'probably was a mere drafting oversight' because 'several African

17 See also E El-Obaid & K Appiagyei-Atua 'Human rights in Africa – A new perspective on linking the past to the present' (1996) 41 *McGill Law Journal* 819-854.
18 Yilma (n 2) 115.
19 Makulilo (n 3) 331.
20 J Swanson 'The emergence of new rights in the African Charter' (1991) 12 *New York Law School Journal of International and Comparative Law* 307-333.
21 Motala (n 6).
22 AB Makulilo *Privacy and data protection in Africa* (2014).
23 AB Makulilo *African data privacy law* (2016).
24 Yilma (n 2) 114.
25 As above.
26 Yilma (n 2) 115.
27 The African Charter is the main regional human rights treaty upon which the African human rights system rests. See M Jimoh 'Investigating the responses of the African Commission on Human and Peoples' Rights to the criticisms of the African Charter' (2023) 4 *Rutgers International Law and Human Rights Law Journal* 1. See also M Mutua 'The Banjul Charter and the African cultural fingerprint: An evaluation of the language of duties' (1995) 35 *Virginia Journal of International Law* 339; M Samb 'Fundamental issues and practical challenges of human rights in the context of the African Union' (2009) 15 *Annual Survey of International and Comparative Law* 61.

countries have had some form of privacy protections in their constitutions and civil laws long before the Banjul Charter was adopted'.[28]

In his response to Yilma, Makulilo capitalises heavily on Yilma's lack of cogent proof that privacy was not a foreign notion from the West. Makulilo states:

> The third misconception about the critique is that it evasively denies the proposition I made in my two books that privacy is an imported concept in Africa. Of course, it is not necessary that Yilma has to agree with me. However, his denial remains normative. It lacks any support of evidence yet the critique wants to romanticise that the notion of privacy is not alien to the African culture. Surprisingly, the critique fails to locate the place of privacy in the African culture and/or identify any society in Africa where the notion of privacy existed or was practiced independently of the influence from the West. My position is somewhat similar to other scholars with regard to the origins of privacy in non-Western cultures.[29]

To buttress his argument, Makulilo then quotes Greenleaf's *Asian data privacy laws: Trade and human rights perspectives*[30] and Bygrave's *Data privacy law: An international perspective*,[31] that privacy is an imported notion to Africa. Makulilo expresses his surprise that Yilma fails to see a clear point from this evidence.[32] On Yilma's accusation that Makulilo briefly considered the absence of a privacy provision in the Africa Charter in his *Privacy and data protection in Africa* and that the omission probably was a mere drafting oversight, Makulilo confronts Yilma with Yilma's joint article with Birhanu published in 2013,[33] where Yilma expresses the view that privacy may be inferred and implied in the African Charter. This sudden shift in position does not sit well with Makulilo, and he remarks that 'in the first instance he argues that privacy in the Charter is implied, in another he argues the absence of the privacy is a mere drafting oversight. This is confusion and lack of academic certainty.'[34]

3 The fallacies in Yilma's review

3.1 The ubuntu fallacy

The first fallacy in Yilma's review is his suggestion that the presence of ubuntu could denote the absence of privacy in [Southern] Africa.[35] Yilma claims that ubuntu 'represents mostly the southern part of Africa'.[36] This is erroneous.

28 Yilma (n 2) 115.
29 Makulilo (n 4) 321-322.
30 G Greenleaf *Asian data privacy laws: Trade and human rights perspectives* (2014).
31 L Bygrave *Data privacy law: An international perspective* (2014).
32 Makulilo (n 3) 322.
33 K Yilma & A Birhanu 'Safeguards of right to privacy in Ethiopia: A critique of laws and practices' (2013) 26 *Journal of Ethiopian Law* 94-152.
34 Makulilo (n 3) 331.
35 Yilma (n 2) 114.
36 As above.

Ubuntu extends beyond the shores of the southern part of Africa. Ubuntu is a core African identity. In the epistemologies of identity, most literature has classified it as an *originary* African identity, and that, just like the *volksgeist* of Germany, ubuntu represents an 'intrinsic core – an organic centre that has always been there'.[37] Although it is argued that the uniqueness of the African culture is not sameness, but diversity,[38] ubuntu represents a general African worldview,[39] even if not called ubuntu throughout Africa. This is because the underlying philosophy of the concept of ubuntu is recognised in the Africa's diverse culture. Among the Yorubas of the Southwestern Nigeria, ubuntu is their concept of *ebi*[40] or *omolúwàbí*.[41] In the Igbo tribe of Southeastern Nigeria, it is their concept of *Ibuanyindanda*.[42] In Angola, ubuntu is their concept of *gimuntu*,[43] Whilst *botho*, *bomoto, vumuntu, umuntu, unhu, ubuthosi,* represent the concept of ubuntu in Botswana, Congo, Malawi, Mozambique, Uganda, the Shona people of Zimbabwe and Ndebele people of Zimbabwe, respectively.[44]

However, it is important to state that the *originary* classification of ubuntu as an African identity, 'a collective true self: an orthodox African sameness, a haecceity or unsullied purity',[45] does not denote its *exclusivity* to the African identity. Ubuntu as a concept embodies some moral principles,[46] and scholars have used different moral words to describe it. For instance, Mugumbate and Nyanguru provide some 17 different words to describe ubuntu.[47] Gade did a study tracing the history and metamorphosis of ubuntu in texts, and posits no less than 32 different words that had been used in literature to describe ubuntu since 1846.[48]

37 C Ngwena *What is Africanness? Contesting nativism in race, culture and sexualities* (2018) 26.
38 M Letseka 'In defence of ubuntu' (2012) 31 *Studies in Philosophy and Education* 48.
39 C Gade 'The historical development of the written discourses on ubuntu' (2011) 30 *South African Journal of Philosophy* 317.
40 T Fagunwa 'Ubuntu: Revisiting an endangered African philosophy in quest of a pan-Africanist revolutionary ideology' (2019) 3 *Genealogy* 5.
41 B Dauda 'African humanism and ethics: The cases of ubuntu and *omolúwàbí*' in A Afolayan & T Falola (eds) *The Palgrave handbook on African philosophy* (2017) 475-491.
42 K Okoro 'Ubuntu ideality: The foundation of African compassionate and humane living' (2015) 8 *Journal of Scientific Research and Reports* 1-9.
43 J Mugumbate & A Nyanguru 'Exploring African philosophy: The value of ubuntu in social work' (2013) 3 *African Journal of Social Work* 85.
44 As above.
45 Ngwena (n 37) 26.
46 T Metz 'Ubuntu as a moral theory and human rights in South Africa' (2011) 11 *African Human Rights Law Journal* 532-559.
47 Mugumbate & Nyanguru (n 43) 85.
48 Gade (n 39) 303-329.

Although words such as kindness,[49] politeness,[50] brotherhood,[51] collectivity[52] and dignity[53] have been used to describe ubuntu, it would be ethnocentric to opine that these virtues are *originary* to Africa in the sense of exclusiveness and xenocentric to contend that the ubuntu theory is unique to South Africa.[54] As an instance, the Universal Declaration of Human Rights (Universal Declaration), the first universal human rights document, talks about the 'recognition of the inherent dignity ... is the foundation of freedom, justice and peace in the world',[55] and that 'all human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.'[56] Van Binsbergen has postulated that dignity and brotherhood are parts of the four attributes of ubuntu,[57] but the none of the diplomats instrumental to the drafting of the Universal Declaration – John Humphrey, Eleanor Roosevelt, Chang Peng-chun and Charles Habib Malik – was African.[58] Aquinas also spoke of the 'common good' in his writings.[59] Thus, it is correct to caution that 'it would be ethnocentric and, indeed, silly to suggest that the ubuntu ethic ... is uniquely African. After all, the values which ubuntu seeks to promote can also be traced in various Eurasian philosophies.'[60]

Admittedly, there is a core principle of ubuntu – the notion of communality – that is not Western. According to Swanson, the notion of communality was abandoned in the West after the emergence of liberalism in the seventeenth and eighteenth century Europe as a reaction to medieval political thought borne out of the writings of Hobbes and Locke.[61] Modern continental European scholars continue to propagate liberalism over communalism in their writings.[62] Yilma seems to have adopted only the communal notion of ubuntu to arrive at the conclusion that Makulilo makes a generalisation that privacy was imported to the whole of Africa, as though Yilma agrees that the presence of ubuntu in (Southern) Africa denotes the absence of privacy in that society. This view is erroneous. Using the Yoruba ethic-nation of Southwestern Nigeria as an example,

49 M Letseka 'African philosophy and educational discourse' in P Higgs and others (eds) *African Voices in Education* (2000) 180.
50 Gade (n 40) 307.
51 WV Binsbergen *Ubuntu and the globalisation of Southern African thought and society* (2002) 34.
52 L Mbigi & J Maree *Ubuntu: The spirit of African transformation management* (1995) 111; Okoro (n 42) 3.
53 Metz (n 46) 532.
54 Makulilo (n 3) 320.
55 Univerdal Declaration Preamble, clause 1.
56 Universal Declaration art 1.
57 Binsbergen (n 51) 34; Fagunwa (n 40) 5.
58 Britannica 'Universal Declaration of Human Rights', https://www.britannica.com/topic/Universal-Declaration-of-Human-Rights (accessed 30 January 2023).
59 P Singh 'Macbeth's three witches: Capitalism, common good and international law' (2012) 14 *Oregon Review of International Law* 61.
60 D Louw 'Ubuntu and the challenges of multiculturalism in post-apartheid South Africa' (2001) 15 *Quest: An African Journal of Philosophy* 28.
61 Swanson (n 20) 325.
62 A Rhodes 'How collective human rights undermine individual human rights' (2020) 227 *The Heritage Foundation* 1-28.

the concept of ubuntu is their notion of *ebi*.[63] In a sociological study of the Yoruba compound conducted by Fadipe and Shitta-Bey, they point out that even within the communal setting of a Yoruba compound, some privacy remained:

> The prevalent form of human dwelling-place in Yorubaland is a collection of apartments for individual families. These apartments together are known as the compound, or to the Yoruba as *agbo ile* (lit, a flock of houses). They consist of two or more rooms for each family – polygynous or monogamous – and adjoin each other, with a common wall between adjacent apartments. The whole collection forms a square enclosing an open space in the middle. A veranda, which opens on to the quadrangle, runs right round the compound and, unlike the rooms behind it, it is not divided by any partition so as to enable inmates to walk from one end of the compound to the other under cover.[64]

From the above, in a typical Yoruba compound, while there was an open space at the centre of the compound, each room was divided by wall – proof of the presence of privacy. In addition, the Yoruba notion of *Àroko* is an exhibition of some privacy. *Àroko* was the traditional system of communication among the Yorubas long before contact with the West.[65] It involves communication using packaged material symbols meant to exclude those who were not steeped in the tradition in which the symbols were used. It was an exhibition secrecy,[66] and such may as well qualify as collective privacy in modern times.[67] Perhaps Yilma does not consider the view that human rights in traditional African societies were strongly based on the 'principle of respect'[68] and that ubuntu is an African world view, and not just a Southern African notion.[69] If he did so, Yilma would probably have made a different inference on the relationship between ubuntu and privacy.

3.2 Lack of proof

Although Yilma posits that privacy was not imported to Africa from the West, he provides no proof, apart from his assertion that 'several African countries have had some form of privacy protections in their constitutions and civil laws long before the Banjul Charter was adopted'.[70] It is true that African countries have had privacy in their constitutions before the adoption of the African Charter in 1986. But this does not *ipso facto* prove Yilma right, namely, that such presence of

63 Fagunwa (n 40) 5.
64 N Fadipe *The sociology of the Yoruba* (1970) 97-98; A Shitta-Bey 'The family as basis of social order: Insights from the Yoruba traditional culture' (2014) 23 *International Letters of Social and Humanistic Science* 79-89.
65 TA Akanbi & OA Aladesanmi 'Shortcut in communication: A case of Àrokò in information and communications technology (ICT)' (2014) 14 *Global Journal of Human-Social Science: G Linguistics and Education* 25.
66 As above.
67 W Hartzog 'What is privacy? That's the wrong question' (2021) 88 *University of Chicago Law Review* 1684.
68 Motala (n 6) 381; Cobbah (n 11) 321; N Sudarkasa 'African and Afro-American family structure: A comparison' (1980) 11 *Black Scholar* 50.
69 Gade (n 39) 317; Cobbah (n 11) 323.
70 Yilma (n 2) 115.

privacy in those constitutions validates the view that privacy was always present in African societies and was not imported to Africa. This is not to say that privacy was imported to Africa. As stated above, there indeed is evidence of the presence of privacy in traditional African societies (or, at least, in the Yoruba ethic nation), even within their communal ontology. Rather, Yilma argues on a false premise, although he arrives at a correct conclusion. The false premise is the assertion that the presence of privacy provisions in several African constitutions before the adoption of the African Charter denotes the presence of innate privacy in these societies. Yet, Yilma was right in his conclusion that there was innate privacy in these societies before contact with the West.

Makulilo exploits Yilma's lack of evidence, stating that Yilma's 'denial remains normative. It lacks any support of evidence yet the critique wants to romanticise that the notion of privacy is not alien to the African culture.'[71] One source showing the recognition of privacy before the adoption of the African Charter is section 22 of the 1960 Nigerian Constitution which guaranteed the right to private and family life. Nevertheless, this does not prove innate privacy in African societies, as Yilma attempts to argue. It should be noted that the presence of privacy in the constitutions of African states before the adoption of the African Charter is as a result of colonial contact with the West, rather than the innate privacy in African societies. Motala posits:

> The constitutions of most independent African countries were initially modelled on, and embodied principles taken from, the constitutions of the colonial powers and the Universal Declaration. For many African countries, acceptance of the constitution drafted by the colonial power was a prerequisite for achieving independence. Admittedly, most African governments have accepted the United Nations Charter and the Universal Declaration. However, to argue that acceptance of the United Nations documents by many African governments is an indication of universal standards, would be merely legalistic and would fail to consider wider factors such as the circumstances surrounding the adoption of the constitution.[72]

Thus, such inclusion in these constitutions does not mean that privacy was innate to African societies. Yilma ought not base his assertion on the presence of privacy in these constitutions. Yet, neither does it mean that privacy was imported from the West to African societies. The reasonable possibility inferred from existing scholarship is that both the West, with its liberalism, and Africa, with its communalism, respected human privacy, since 'there may be some common beliefs and values (*like privacy*)',[73] even though their conceptualisation of these values might be different.[74] The notion of privacy in the two societies, albeit present in both, was conceived differently. This difference in conception of what privacy meant and its scope neither changes the assertion that privacy existed in

71 Makulilo (n 3) 322.
72 Motala (n 6) 378.
73 My emphasis. See R D'sa 'Human and peoples' rights: Distinctive features of the African Charter' (1985) 29 *Journal of African Law* 72-81.
74 El-Obaid & Appiagyei-Atua (n 17) 829-830.

African societies before contact with the West nor does it mean that the West is the originator of privacy.

It is interesting that a society that Yilma – having an Ethiopian origin – could have used as proof that privacy existed in pre-colonial African societies is the Amhara community of Ethiopia. According to Levine, 'the Amhara ... maintain a high degree of respect for privacy, despite the hierarchy character of their society'.[75] Levine states that in this community, 'the individual home is regarded with great respect' and that 'no one, not even a relative, presumes to enter another's home without being properly acknowledged or escorted inside'.[76] The privacy notion in this community is premised on the view that no one has 'a just claim to information about one's person'.[77]

3.3 Omission of privacy in the African Charter as an oversight

Further, Yilma is of the view that the absence of privacy in the African Charter is an 'omission' which 'probably was a mere drafting oversight'.[78] This proposition is so critical and could only be made when the jurisprudence behind the African Charter is not considered. Articles such as 'Human and peoples' rights: Distinctive features of the African Charter' by D'sa; 'The African Charter on Human and Peoples' Rights: A legal analysis' by Gittleman;[79] 'The protection of human rights in Africa and the African Charter on Human and Peoples' Rights: A comparative analysis with the European and American systems' by Okere; 'A critique of the African Charter on Human and Peoples' Rights' by Bondzie-Simpson;[80] 'Human rights in Africa: A cultural, ideological, and legal examination' by Motala; and Swanson's 'The emergence of new rights in the African Charter', all underscore the distinctiveness of the African Charter which, if considered by Yilma, would have caused him to abandon the thought that privacy was omitted in the African Charter as a result of an oversight.

The assignment of the drafters of the African Charter was straightforward: They 'were entrusted with the mandate of preparing an African Charter on Human and Peoples' Rights which "reflects the African conception of human rights"' and were instructed to 'take as a pattern the African philosophy of law and meet the needs of Africa'.[81] The reason for this deliberate quest to ensure that the African Charter contains human rights grounded in African custom and tradition is shared by many scholars.[82] According to Swanson:

75 DN Levine *Wax and gold: Tradition and innovation in Ethiopian culture* (1972) 264.
76 As above.
77 Levine (n 75) 265.
78 Yilma (n 2) 115.
79 R Gittleman 'The African Charter on Human and Peoples' Rights: A legal analysis' (1982) 22 *Virginia Journal of International Law* 667-714.
80 E Bondzi-Simpson 'A critique of the African Charter on Human and Peoples' Rights' (1988) 31 *Howard Law Journal* 643.
81 D'sa (n 73) 73.
82 See, eg, Gittleman (n 79) 667-714; Swanson (n 20) 307-333; Motala (n 6) 373-410.

> Many Africans believed that at the time the Universal Declaration and the International Covenants were drafted most of the member states of the United Nations were states 'with white populations and largely Christian traditions'. Therefore, they were determined to create a uniquely African document more responsive to African needs.[83]

The African Charter mirrors traditional African values.[84] Therefore, where it markedly differs from other international human rights instruments, such difference should not be hastily labelled as an oversight but must first be considered in light of African customs before a conclusion is made. Using the analogy of the absence of a court in the African Charter as an example,[85] the African Court on Human and Peoples' Rights was not included in the African Charter, but was established in 2006[86] after the required number of ratifications needed for the Protocol establishing it was completed in 2004.[87] Should it be concluded that the absence of the African Court in the African Charter probably also was a mere drafting oversight? Notable human rights scholars such as Swanson and Murray maintain that the reason for the absence is because the drafters 'insisted that this feature, *like much of the Charter*, is more suited to traditional methods of settling disputes through friendly arbitration than to the adversarial approach of the West'.[88] Therefore, since the African Charter is unique, it is necessary to consider whether the absence of a privacy provision is also *like much of the Charter* before concluding that the omission was an oversight. Much of the available evidence supports the proposition that the absence of a privacy provision was deliberate, rather than an oversight.

Support for the conclusion in the preceding paragraph may be found when one considers the *travaux préparatoires* of the African Charter. Generally, the African Charter is said to have a few available *travaux préparatoires*.[89] However, several scholarships have asserted that the first draft of the African Charter – prepared by Keba M'baye – contained a privacy provision.[90] Subsequently, several

83 Swanson (n 20) 327.
84 African Charter Preamble, art 4; Okere (n 14) 145.
85 This analogy had been used in Jimoh (n 27).
86 See TG Daly & M Wiebusch 'The African Court on Human and Peoples' Rights: Mapping resistance against a young court' (2018) *International Journal of Law in Context* 294.
87 NB Pityana 'Reflections on the African Court on Human and Peoples' Rights' (2004) 4 *African Human Rights Law Journal* 121. Prior to the establishment of the African Court, the African Commission served as the only [quasi] judicial body to address claims of violation of the African Charter since 1987. See M Jimoh 'A critique of the seizure criteria of the African Commission on Human and Peoples' Rights (2022) 22 *African Human Rights Law Journal* 364.
88 Swanson (n 20) 330. R Murray & D Long 'Monitoring the implementation of its own decisions: What role for the African Commission on Human and Peoples' Rights' (2021) 21 *African Human Rights Law Journal* 837.
89 See MA Plagis & L Riemer 'From context to content of human rights: The drafting history of the African Charter on Human and Peoples' Rights and the enigma of article 7' (2021) 25 *Journal of History of International Law* 563.
90 YE Ayalew 'Untrodden paths towards the right to privacy in the digital era under African human rights law' (2022) 12 *International Data Privacy Law* 26.

other drafts[91] were introduced by African states and groups during seminars and conferences, which excluded privacy. For this reason, notable scholars such as Viljoen and Murray submit that 'it appears that the right to privacy was left out of the Charter deliberately'.[92] While it is unclear why privacy was excluded from the available *travaux préparatoires,* one persuasive reason is that 'the drafters felt that the privacy contained in other international human rights treaties that preceded the Charter was more Western oriented, which was thought to be too individualistic and contrasted with the communalistic foundation of the Charter'.[93] This indeed arguably better explains the absence of privacy in the African Charter, rather than Yilma's critical assertion that it was mistakenly omitted.

4 The fallacies in Makulilo's response

This article considers three fallacies in Makulilo's response below.

4.1 Evidence but unreliable evidence

Makulilo criticises Yilma in the following words:

> Surprisingly, the critique fails to locate the place of privacy in the African culture and/or identify any society in Africa where the notion of privacy existed or was practiced independently of the influence from the West. My position is somewhat similar to other scholars with regard to the origins of privacy in non-Western cultures.[94]

There are two issues here. First, Yilma's failure to provide evidence of where the notion of privacy existed independently of the influence from the West does not validate Makulilo's view that privacy originated from the West. Second, Makulilo proceeds to present his own evidence citing two scholars who, according to Makulilo, underscore his view that privacy is a Western notion. Makulilo quotes Greenleaf's *Asian data privacy laws: Trade and human rights perspectives* who argues in his book:

> Are *data privacy* laws legal transplants? *Data privacy laws* originated as a 'Western' notion, in that their earliest legislative instantiations were in North America (1970 and 1974), and in seven Western European countries in the 1970s. Furthermore, the principal players who negotiated their transformation into an international

91 For discussion on the debates and drafts, see AB Akinyemi 'The African Charter on Human and Peoples' Rights: An overview' (1985) 46 *Indian Journal of Political Science* 207-238.

92 R Murray & F Viljoen 'Towards non-discrimination on the basis of sexual orientation: The normative basis and procedural possibilities before the African Commission on Human and Peoples' Rights and the African Union' (2007) 29 *Human Rights Quarterly* 89.

93 Jimoh (n 27). See also A Ibidapo-Obe *Essays on human rights law in Africa* (2005) 260; O Ogbu *Human rights law and practice in Nigeria* (2013) 280-281.

94 Makulilo (n 3) 322.

> standard, the OECD Guidelines, in 1978-80 were from Europe, North America, and Australasia.[95]

After quoting Greenleaf, Makulilo states that 'the above passage clearly provides that *privacy* is not indigenous to any Asian country. Both the concept and its regulation are imported from the West. This is true to other non-Western cultures including Africa.'[96] Makulilo thereafter quotes Bygrave's *Data privacy law: An international perspective*, where Bygrave expresses the following view:

> The development of *data privacy law* in Africa reflects multiple factors. These include: a desire to meet the adequacy requirements of DPD articles 25-26 and thereby attract foreign investment, particularly in the use of local outsourcing industry; recent first-hand experience of political oppression; the requirements of ICCPR article 17; and old lines of colonial influence. [97]

I was lost for a moment after reading Makulilo's view. His debate with Yilma is about the origin of *privacy* in Africa and not the origin of *data privacy* in Africa. These two concepts are entirely different. Greenleaf's and Bygrave's books quoted by Makulilo as his proof that privacy was imported from the West to Africa underline the origin of *data privacy,* and not the origin of *privacy* in Africa, which is the purport of Makulilo's debate with Yilma. Roos, one of African's early academic scholars in the field of data privacy, has made the point in one of her papers – 'Privacy in the Facebook era: A South African legal perspective' –that data privacy is a narrower concept than privacy.[98] In her words, 'data protection law is related to privacy, but is a narrower concept in that it relates only to the processing of personal information'.[99] Roos cites Christopherm, whose view is the following:

> Privacy includes issues relating to the protection of an individual's 'personal space' *that go beyond data protection*, such as 'private, family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection against misuse of private communications, protection from disclosure of information given or received by the individual confidentially'.[100]

It is interesting to note that Makulilo cites this Roos's article in his response to Yilma's review and even accords respect to Roos, stating:

> I am aware early African academic scholars in the field of data privacy such as Professor Anneliese Roos who graduated with her PhD degree at the University of South Africa in 2003 has not stopped conducting research in this field. One of

95 Greenleaf (n 30) 12; see Makulilo (n 3) 322.
96 As above.
97 Bygrave (n 31) 106; Makulilo (n 3) 322-323.
98 A Roos 'Privacy in the Facebook era: A South African legal perspective' (2012) 129 *South African Law Journal* 375.
99 As above.
100 K Christopher 'An international legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law and Security Review* 307-317; see Roos (n 98) 375.

her recent publications that has addressed the challenges of modern technology is *Privacy in the Facebook era: A South African legal perspective*. Roos has authored chapter 9 of the *African data privacy laws*. Could this and, according to Yilma, place Roos in the second generation?[101]

Perhaps Makulilo mistakenly misses this point in Roos's paper. This then leaves one to the conclusion that Makulilo falls into the same fallacy for which he criticises Yilma: He too does not provide evidence that *privacy* originated from the West. Clearly, the Greenleaf and Bygrave evidence relied on by Makulilo in support of his assertion that privacy is a Western concept at best is evidence that data privacy may be a Western concept, but it is not evidence that privacy is a Western concept.

4.2 The individualistic–communalistic argument

Notwithstanding Makulilo's lack of evidence on the importation of privacy from the West, he, unlike Yilma, has been consistent in his views about privacy in Africa. In as article published in 2016,[102] Makulilo posits that traditional African society did not recognise the concept of privacy, a situation he termed 'privacy myopia'.[103] He refers to traditional African society as the pre-colonial period – a period before contact with the West.[104] Using the Neethling theory – which he states to have been adopted by the Supreme Court of Appeal of South Africa[105] – Makulilo argues that the individualistic nature of privacy contrasts with the communalistic nature of traditional African society and that it is safe to argue that 'privacy in Africa is principally a Western imported liberal concept'.[106] However, what is missing in Makulilo's view is that privacy involves some measure of space creation[107] and this is found in all societies, including in Africa, before contact with the West. The examples of the Yoruba society in Nigeria and the Amhara community of Ethiopia described above are proof of this exertion.[108] Of course, this is not to suggest that all forms of space creation imply privacy, but certainly privacy in all its forms connotes space creation. Roos has made this point in her writings.[109]

In recent times, the individualistic-communalistic argument about privacy is waning. This is because there are several reasons why it is fallacious to assert that privacy cannot exist in a communalistic society. First, such assertion tends to portray the view that individual rights cannot exist in a communal setting. Yet, individual rights are protected in communal societies. According to Taylor,

101 Makulilo (n 3) 334.
102 Makulilo (n 8).
103 Makulilo (n 8) 193.
104 Makulilo (n 8).
105 Makulilo (n 8) 196.
106 Makulilo (n 8).
107 Roos (n 19) 555.
108 Fadipe (n 64); Shitta-Bay (n 64); Levine (n 75).
109 Roos (n 8) 556.

the choice is not always between a close, family-like community and a modern, impersonal society since it is possible to have a 'communitarian or holist ontology and to value liberalism's individual rights'.[110] Second, there is the 'societal dimension of privacy'. In any society – whether individualist or communalistic – 'individual privacy has a social value because protecting it contributes to societal goals'.[111] For these reasons, there were several values to be protected with the respect of privacy rights in African societies before contact with the West.

I suppose Makulilo's view that traditional African society did not recognise the concept of privacy emanates from equating autonomy with privacy. The communalistic nature of traditional African society erodes autonomy, and not privacy. Roos gives a clear distinction between these two concepts in her PhD thesis. She posits that autonomy is when there is a prescription on how to manage private lives. In this case, 'it is not privacy that is involved here', states Roos, 'but the individual's right to freely exercise his or her will, that is his or her autonomy, or the capacity to live one's life as one chooses'.[112]

The thesis of this article is that the communalistic nature of the traditional African society affects individual autonomy, and not privacy, which some scholars even consider innate to all humans.[113] According to a researcher's experience while conducting biomedical research in a rural community in the Northern KwaZulu-Natal province of South Africa:

> For me to talk to the mother and the child, the granny and the father must give me permission. It means now, they are the ones who are allowing that person, so that person is not, there is no *autonomy* in her because she is not allowed to decide whether she wants it or not. She must first get consent from these two other people or the mother-in-law, must say yes or no or even father-in-law. You see, so that her autonomy is affected. She cannot voluntarily say no I am going to take part. She has got to wait for husband or *gogo* [grandmother] or mother-in-law, you know.[114]

The foregoing underscores a situation where the autonomy of the subject is eroded, and not the privacy of the subject. Using the Neethling theory, one may find that the subject had some aspects of their life private from their father, mother or grandmother. Also, the marital bedrooms of pre-colonial Africa had 'sacred precincts', and it would be absurd to argue that there was no privacy in Africa before contact with the West. Pre-colonial Africa had a practice where the families of couples and villagers only knew of the virginity status of the wife when the husband publicly disclosed what went on in sacred precinct of the

110 C Taylor 'Cross-purposes: The liberal-communitarian debate' in N Rosenblum (ed) *Liberalism and the moral life* (1991) 161.
111 DJ Solove 'The limitations of privacy rights' (2023) 98 *Notre Dame Law Review* 987.
112 Roos (n 8) 559.
113 See, eg, E Neill *Rites of privacy and the privacy trade: On the limits of protection for the self* (1962) 36.
114 F Akpa-Inyang & SC Chima 'South African traditional values and beliefs regarding informed consent and limitations of the principle of respect for autonomy in African communities: A cross-cultural qualitative study' (2021) 22 *BMC Medical Ethics* 9.

marital bedroom on the wedding night. Virginity testing is a private matter in pre-colonial Africa, unless announced publicly.[115]

The Yorubas, for instance, also have several proverbs depicting that privacy was a value in their societies. The saying *ile eni lati n je ekute onidodo* – which literally means 'it is in one's house that one eats a rat with abdomen' – is used to describe a situation where one intends to keep a situation private. Several other sociological studies describing the Yoruba architectural courtyard state that privacy was an important value that influenced the design.[116] Beyond the Yorubas, the African house has been described as being rooted in 'principles of privacy and spatial comfort'.[117] Specifically, studies describing the Benin houses conclude that 'the spatial arrangement of spaces in Benin houses has spaces for private and collective use'.[118] The *Zaure* in Hausaland also depicts the respect for privacy in this society before contact with the West. The *Zaure* is a place for guest reception.[119] Describing a traditional Hausa residence, Umar and others state:

> A traditional Hausa residence is conceptually subdivided into (3) parts or layout, inner core (private area), a central core (semi-private area), and outer core (public areas) ... These concepts historically originated from Egyptian domestic architecture of around (500 CE). Hence, Hausa traditional village layouts of shelter and settlements that developed to villages and town in such morphology.[120]

Further, a study analysing the traditional courtyard houses in Nigeria – in the Yoruba, Igbo and Hausa cultures – reveals that privacy is a main influence in the design of these courtyards.[121] Thus, evidence abounds – which may be found in proverbs, architectural designs, customary laws – showing that traditional African societies respected privacy within their communal ontology before contact with the West.

4.3 *Ad hominem*

Makulilo also commits *ad hominem* in his reaction to Yilma's critique that he briefly mentions the absence of privacy in the African Charter in his book *Privacy and data protection in Africa*. Makulilo fails to address Yilma's critical view that the

115 OW Ogbomo & QO Ogbomo 'Women and society in pre-colonial Iyede' (1993) 88 *Anthropos* 437.

116 A Adedokun 'Incorporating traditional architecture into modern architecture: Case study of Yoruba traditional architecture' (2014) 11 *British Journal of Humanities and Social Sciences* 39-45, 42; TM Adebara 'Private open space as a reflection of culture: the example of traditional courtyard houses in Nigeria' (2023) 48 *Open House International* 617-635.

117 AE Ikudayisi & TO Odeyale 'Designing for cultural revival: African housing in perspective' (2021) 24 *Space and Culture* 630.

118 CO Adeokun, EN Ekhaese & F Isaacs-Sodeye 'Space use patterns and building morphology in Yoruba and Benin' (2013) Proceedings of the Ninth International Space Syntax Symposium 20.

119 Ikudayisi & Odeyale (n 117) 625.

120 GK Umar and others 'The practice of Hausa traditional architecture: Towards conservation and restoration of spatial morphology and techniques' (2019) 5 *Scientific African* 3.

121 Adebara (n 116).

absence of privacy in the African Charter probably was a mere drafting oversight. Instead, Makulilo confronts Yilma with Yilma's earlier contrary view. He states:

> He (Yilma) complains that I made brief mention of the absence of the right to privacy in the African Charter ... In their joint article Yilma and Birhanu had previously assigned a different reasoning to account for the lack of a privacy provision in the ACHPR: 'Although the African Charter on Human and Peoples' Rights (hereinafter the African Charter) does not explicitly say anything about the right to privacy, one may argue that some aspect of privacy is impliedly enshrined in it when the Charter stipulates that (art 5): And hence, such aspect of privacy can be inferred from the African Charter.' This is evidence that Yilma has always been contradictory of his earlier opinion. In the first instance he argues that privacy in the Charter is implied, in another he argues the absence of the privacy is a mere drafting oversight. This is confusion and lack of academic certainty.[122]

Like Yilma, Makulilo does not explain why privacy was omitted in the African Charter. With due respect, the whole response of Makulilo to Yilma's review of chapter 5 of Makulilo's book, *Privacy and data protection in Africa,* makes one wonder whether Makulilo is trying to make Westerners out of Africans in respect of the origin of privacy in Africa.

5 Conclusion

This article wades into the debate started by Alex B Makulilo and Kinfe M Yilma on the origin of privacy in Africa. While the article agrees with Yilma that the notion of privacy was not alien to Africa before contact with the West, it solidifies this claim by providing evidence, an exercise lacking in Yilma's review. The article argues that within the communal ontology of pre-colonial African societies, privacy existed. In addition, the article interrogates some other aspects of the Makulilo-Yilma debate, especially the relationship between ubuntu and privacy and the claim that the absence of privacy in the African Charter probably was 'a mere drafting oversight'. It finds that the presence of ubuntu in African societies does not denote absence of privacy. It also argues that the absence of a privacy provision in the African Charter was not a drafting oversight, but a deliberate effort to exclude privacy, which was understood as individualistic at the time of drafting the African Charter, from a communalistic treaty such as the African Charter. The drafting history of the African Charter shows that the right to privacy was initially considered despite being subsequently abandoned. Therefore, its absence in the African Charter could not have been an oversight. The article also finds that Makulilo – the chief proponent of the idea that privacy was imported to Africa from the West – has provided no proof to such claim. The article argues that the evidence provided by Makulilo shows that data privacy was imported to Africa, and not privacy.

122 Makulilo (n 3) 331.

African Journal on Privacy & Data Protection

To cite: J Wanjiku & T Khaoma 'A case for continental cooperation in the harmonisation of a regional legal framework for cross-border data transfers in Africa' (2024) 1
African Journal on Privacy & Data Protection 18-49
https://doi.org/10.29053/ajpdp.v1i1.0003

A case for continental cooperation in the harmonisation of a regional legal framework for cross-border data transfers in Africa

*Joy Wanjiku**
Advocate of the High Court of Kenya

*Taria Khaoma***
Advocate of the High Court of Kenya

Abstract:

The widely cited analogy "data is the new asset" or "data is the new commodity" underscores the fundamental role of personal data in today's economic context. This was observed in the increase in the uptake of digital technologies and solutions that relied heavily on personal data following the COVID-19 pandemic. We live in a world where an individual's data collection takes place in one jurisdiction, and is processed and retained in another jurisdiction. Transferring personal data across international borders is a crucial element of the digital economy. Despite the benefits that would accrue to national economies and businesses by allowing data flows in the African region, African countries either do not have regulations

* Bachelor of Laws, Strathmore University and an Advocate of the High Court of Kenya. Commercial, Employment and IPT Associate at DLA Piper Africa, Kenya (IKM Advocates).
** Bachelor of Laws, Strathmore University. Advocate of the High Court of Kenya and member of the International Association of Privacy Professionals (IAPP). IP and TMT Associate at Bowmans Kenya (Coulson Harney LLP).

in place to address cross-border data transfers or have taken different approaches to regulation. Certain nations mandate that foreign countries adhere to specific minimum data privacy standards before allowing the transfer of data across their respective borders. The common standard of cross-border data transfers has been an adequate level of data protection by the recipient country, but what is an adequate level of data protection? The unforeseen result of these fragmented measures is the localisation of data, primarily because of the variations in how countries safeguard data, or the recipient's incapacity to guarantee the sender that they will adequately protect the data of their citizens.

Key words: data localisation; African Union; cross-border data transfer; adequacy decisions; data protection

1 Introduction

For centuries information has been circulating worldwide, and the means of transmission have evolved with time from international mail to transatlantic cables, subsequently to telephone cables. As digital transformation continues to spread across nations and industries, data flows are expected to surge even more.[1] In the modern data-driven world, cross-border data transfers have become an essential part of the global economy. The movement, storage and processing of data across borders serve as a foundational pillar for contemporary international trade and investments. This critical infrastructure bolsters the swift expansion of digital services and enterprises across the world.

In the throes of the COVID-19 pandemic, from 2020 to 2021, the global community depended heavily on international data transfers to synchronise economic operations both domestically and globally, alleviate the negative impacts on trade, and sustain essential value networks.[2] The occurrence of such events has underscored the pivotal role of cross-border data sharing in ensuring the continuity of a free market, where willing sellers and willing buyers can efficiently engage in commerce, making informed decisions, and facilitating global economic interactions. However, with the increase in data flows, concerns around data privacy, security, and protection have arisen, leading to various regulatory approaches across different regions.

Cross-border data flows encompass the transfer and movement of data or information between servers across the borders of distinct sovereign entities

1 N Cory & L 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), https://d1bcsfjk95uj19.cloudfront.net/sites/default/files/2021-data-localization.pdf (accessed 13 March 2023).

2 F Cilauro, S Snelson & A Breckenridge 'The economic impact of cross-border data flows' 17 June 2021, https://www.frontier-economics.com/uk/en/news-and-articles/news/news-article-i8493-the-economic-impact-of-cross-border-data-flows/# (accessed 23 September 2023).

using network equipment designed for such transmission.[3] These data flows empower individuals to convey information for online communication, monitor international supply chains, exchange research, offer services across borders, and foster technological advancements. The necessity of cross-border data transfers can vary depending on the agreements among data processors, controllers, owners, recipients, and the specific objectives behind such data transfers.[4]

In Africa there has been a significant shift in the realm of personal data protection following the introduction of the General Data Protection Regulations by the European Union (EU). This shift has spurred the adoption of local and regional regulations on data privacy across Africa, including the ECOWAS Data Protection Act in 2010, the East Africa Community Legal Framework for Cyber Laws in 2010, and the Southern African Development Community Model on Electronic Transactions and Electronic Commerce.[5]

Considering the afore-mentioned, cross-border data transfers have become a complex issue due to the different approaches to data protection, leading to disjointed measures and unintended consequences, such as data localisation. Presently, African governments are leaning on their own national data protection regulations, and cross-border data transfers are particularly allowed contingent upon the existence of appropriate safeguards and data protection regulations in the recipient state that ensure the protection of personal data. Furthermore, the level of control over cross-border data transfers within free trade agreements (FTAs) and preferential trade agreements (PTAs) in Africa varies widely. Some of the current provisions pertain to data protection in cross-border transfers, whereas others make no reference to this aspect at all.[6]

The absence of a harmonised framework on cross-border data transfers has hindered the free flow of data in Africa, resulting in negative consequences for businesses and the economy at large. When there is a legislative gap, the personal data of consumers, who are the data subjects, becomes vulnerable to potential compromise and attacks from cybercriminals, identity theft, unauthorised access by foreign surveillance and law enforcement agencies, and other risks. These individuals may not receive the necessary recourse or protection.[7] Therefore, for a region that has no model to govern the free flow of data across borders, there is a dire need for continental cooperation and development of a regional legal framework to govern cross-border data transfers, given the potential benefits to

3 Congressional Research Service 'Data flows, online privacy, and trade policy' (2020) https://sgp.fas.org/crs/misc/R45584.pdf (accessed 23 September 2023).

4 N Rotich 'Examining cross-border data flows provisions in Africa's free trade agreements' 31 August 2023, https://cipit.strathmore.edu/examining-cross-border-data-flows-provisions-in-africas-free-trade-agreements/ (accessed 23 September 2023).

5 C Ewulum 'The legal regime for cross-border data transfer in Africa: A critical analysis' LLB dissertation, University of Nigeria, 2023 4, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4546964 (accessed 23 September 2023).

6 Rotich (n 4).

7 Ewulum (n 5) 5.

national economies and businesses. As per the United Nations (UN) Conference on Trade and Development (UNCTAD), 'effective data protection is closely intertwined with digital trade in goods and services, as inadequate safeguards can erode consumer confidence, leading to adverse market consequences'.[8]

This article underscores the significance of cross-border data transfers, emphasising its abundance, while also considering the obstacles to such transfers, with a specific focus on data localisation. Additionally, the authors highlight how the absence of a unified legal framework for cross-border data flows has hindered the realisation of digital economy advantages. Consequently, the article contends that the African Union (AU) should assume a leading role in establishing a continental legal framework that strikes a balance between data protection and privacy concerns and the advantages of a fluid digital economy. By addressing the present state of cross-border data transfers in Africa and advocating a cohesive legal framework, the article aims to foster continental collaboration, ultimately benefiting national economies and businesses.

2 The roadmap of cross-border data transfers

The growing importance of data in today's digital economy has led to a significant increase in cross-border data transfers. However, this process is not without its challenges. Various legal, technical, and cultural barriers can impede the smooth flow of data across borders. This roadmap of cross-border data transfers draws attention to the series of steps that need to be taken to ensure the safe and secure transfer of data between countries. It begins with the creation and implementation of strong data protection legislation, which includes data security requirements for both public and private sector organisations; the issuance of consent where necessary; ensuring that safeguarding measures are in place for both parties; and receipt of the data.

To facilitate cross-border data transfers, policy makers and industry leaders have developed a roadmap that outlines the key steps necessary for the seamless and secure movement of data between countries. This roadmap includes measures such as binding corporate rules, standard contracts, adequacy decisions, data localisation requirements, data security regulations, and cross-border data transfer agreements. In this part we explore the roadmap of cross-border data transfers and examine the various steps involved in ensuring that data is transferred safely and efficiently across borders.

8 As above.

2.1 Why must data be moved across borders?

Data lacks the attributes of scarcity typically associated with tangible goods or services, as it possesses the inherent qualities of shareability, reusability, and non-depletion.[9] The cross-border transfer of data is a critical component of the digital economy, enabling businesses to operate across borders, facilitating global collaboration, and supporting the adoption of digital technologies. As technological transformation progresses, the collection and processing of data is accelerating through machine-learning products and services such as artificial intelligence and internet of things that are increasingly able to produce, store and analyse an unprecedented amount of data without human intervention.[10] Global data flows are a consequence of the increasing trends of globalisation and digitalisation in business and society, forming a vital foundation for the modern economy. The ability to utilise, share and access information across international boundaries not only stimulates creativity but also empowers the creation of data-driven products and services, driving economic growth and nurturing the generation of new concepts. Furthermore, it often serves as an essential resource for remote communities.[11]

The African Continental Free Trade Agreement (AfCFTA) is centred around economic integration and the promotion of trade whilst carrying significant data protection considerations. One of its primary objectives is the creation of a single market for goods, services, facilitated by movement of persons in order to deepen the economic integration in Africa.[12] AfCFTA aims to enable the unrestricted movement of goods, services and individuals across African borders, inevitably leading to the exchange of data as businesses partake in cross-border transactions. In order to ensure the seamless functioning of AfCFTA, it becomes essential to establish a unified data protection framework for effectively managing cross-border data flows while upholding data privacy laws and regulations. While recognising the state parties' authority to regulate their territories and pursue legitimate policy goals, AfCFTA is also mindful of the importance of creating explicit, transparent, predictable, and mutually beneficial regulations to govern trade in goods and services, competition policy, and intellectual property investment.[13]

Moreover, from a cybersecurity perspective, some states may believe that data is more secure when it is stored within its national borders. However, cross-border data transfers are critical to cybersecurity partly because they allow for

9 United Nations Development Programme 'Enabling cross-border data flow in ASEAN and beyond' (2021), Enabling-cross-border-data-flow-asean-and-beyond-report.pdf (accessed 23 September 2023).
10 As above.
11 Centre for Information Policy Leadership 'Cross-border transfer mechanisms' (2015), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cross-border_data_transfers_mechanisms_cipl_white_paper.pdf (accessed 23 September 2023).
12 African Continental Free Trade Agreement 2018 art 3(a).
13 Ewulum (n 5) 28.

cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data.[14] Storing all data in one geographical territory, contrary to allowing cross-border data flows, reduces risk detection, assessment and response to cyberthreats in a particular country.[15] When governments mandate localisation or restrict the ability to transfer and analyse the free flow of data, the onus of maintaining the security of data becomes a core function of the data controller or data processor. Security is determined by the technical, administrative and operational protections, put in place by the service provider, that accompany the data, not the location.[16] Therefore, regardless of whether or not governments impose data localisation requirements, it might not necessarily mitigate a security breach.

By limiting the flow of data across borders, the process of detecting suspicious activities becomes more complex. Criminals can exploit gaps in cross-border data sharing to commit crimes such as fraud, money laundering and terrorism financing. 'A criminal rejected in one country can open a mobile money account and make transactions in another country.'[17] In order to ensure a robust national security system across a geographically dispersed network, policy makers need to avoid misguided frameworks that limit the default flow of data. However, it is also important to strike a balance between cross-border data sharing and data protection. While an open and unrestricted flow of data can facilitate crime detection and prevention, it can also compromise data security and privacy. In addition, localising data in one system may lead to lower investment in security and create vulnerabilities that can be exploited by cybercriminals.

2.2 The pathway for moving data across borders

To facilitate the safe and secure transfer of data, several conditions must be fulfilled. These conditions encompass setting a baseline level of data protection; giving cybersecurity a high priority; binding corporate rules; the presence of adequacy decisions and consent from data subjects ensuring hardware accountability across nations; as well as prioritising technical interoperability, data portability and data provenance. Furthermore, it is crucial to ensure that the policy environment is future-proof, so it remains effective and relevant as technology evolves.

14 Global Data Alliance 'Cross-border data transfers and cybersecurity', https://globaldataalliance.org/issues/cybersecurity/ (accessed 30 March 2023).

15 World Economic Forum 'A roadmap for cross-border data flows' (2020), https://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf (accessed 23 September 2023).

16 Cory & Dascoli (n 1) 13.

17 C Scharwatt 'The impact of data localisation requirements on the growth of mobile money-enabled remittance GSMA' (2019), https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf (accessed 23 September 2023).

2.2.1 Establishing an adequate level of data protection

Cross-border transfers of data should generally be permitted under national legislation to enhance trust and allow for regulatory compliance across borders. Almost 72 per cent of countries have full or draft legislation on data protection and privacy. To date, 36 out of 54 African countries have data protection laws and regulations, with 16 countries having signed the Malabo Convention and 13 countries having ratified it.[18] As expected, these laws governing the collection, processing and transfer of data, be it personal identifiable information or sensitive personal identifiable information, vary from country to country.[19] Despite the diverging data protection regulations, there are core principles of data protection that remain fairly consistent from jurisdiction to jurisdiction. These principles include fair and lawful processing of data; purpose specification; minimality; quality; transparency; data subject participation; sensitivity; confidentiality; and accountability. Any differences that may appear are significant to whether a particular data protection law will be a hard or a soft barrier to cross-border data transfer.[20]

When establishing an adequate level of data protection, UNCTAD states that when it comes to cross-border data transfers, countries have either one-off or ongoing exceptions.[21] In one-off exceptions, including allowing the data transfer based on performance of a contract between the data subject and the data controller or the data controller and the data subject, the transfer is based on the exercising of a legal right, and the transfer is necessary in order to protect the vital interests of the data subject. On the other hand, ongoing exceptions include the adequacy approach, where a regulator in a particular jurisdiction issues a whitelist of countries with a sufficient degree of protection that allows for the transfer of personal data. The issuance of white-list countries with sufficient data protection laws has been seen in the EU.

Second, another ongoing exemption approach is the implementation of binding corporate rules by multinational companies. These rules are established as enforceable internal guidelines for handling cross-border data transfers within the company group. This enables multinational corporations to share personal

18 A Sylla 'Recent developments in African data protections laws' 24 February 2023, https://www.engage.hoganlovells.com/knowledgeservices/news/recent-developments-in-african-data-protection-laws-outlook-for-2023 (accessed 18 March 2023).

19 General Data Protection Regulation (EU) 2016/679 of 2016 sec 4. 'Personal identifiable information' means any information relating to an identified or identifiable natural person such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. 'Sensitive personal identifiable information' means all personal data including racial, political, religious, trade union membership, genetic, biometric, sexual orientation, and health details of individuals.

20 World Economic Forum (n 15) 22.

21 United Nations Conference on Trade and Development 'Data protection regulations and international data flows: Implications for trade and development' (2016), https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (accessed 25 September 2023).

data internationally among their group entities, even when the destination country lacks sufficient data protection measures.[22] The binding corporate rules approach differs from the standard clauses approach, which relies on specific contract language to ensure an adequate level of data protection during transfers. Standard contract clauses typically are effective for smaller companies and when data sharing occurs between only two parties.

Furthermore, in some jurisdictions consent has been used as the foundation for cross-border data transfers. This approach hinges on individuals willingly and explicitly providing their consent for their data to be transferred beyond a specific jurisdiction. However, in most cases, relying on consent for cross-border data transfers is subject to additional conditions and requirements.

Therefore, the question arises as to how we can facilitate cross-border data transfers whilst establishing an adequate level of data protection. Data privacy concerns can be addressed by governments through mandating contractual commitments that require parties to adhere to core privacy principles during transfer of data.[23] In this way, regulators are able to enforce partial restrictions that may be helpful to ensure sufficient levels of data protection abroad, they can also hold data transferring companies responsible for consequences caused and are able to apply and enforce national laws against foreign companies. The challenge around protective contracts is that if not harmonised regionally, every country then requires its own contract with its own clauses, causing an undue burden on international trade by requiring multi-nationals to constantly review and execute millions of contractual terms.

2.2.2 Prioritising cybersecurity and jurisdictional accountability

Cybersecurity involves taking steps to protect data from unauthorised access, commonly referred to as cyber attacks. These measures are designed to ensure that data being transferred is received only by its intended recipient and not intercepted or accessed by unauthorised parties.[24] Companies may choose to store data at geographically-diverse locations to obscure the location of data and reduce the risk of physical attacks. Additionally, this enables companies to reduce

22 Price Waterhouse Coopers 'Binding Corporate Rules. The General Data Protection Legislation' https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf (accessed 25 September 2023).

23 World Economic Forum (n 15) 23.

24 A Beyleveld & F Sucker 'Cross-border data flows in Africa: Policy Considerations for the African Continental Free Trade Area Protocol on Digital Trade' Centre for the Studies of Economies of Africa (2022), https://cseaafrica.org/wp-content/uploads/2022/10/2022-10-28-CSEA__MI__Report-on-Cross-Border-Data-Flows-in-Africa__Policy-Considerations-for-the-AfCFTA-Protocol-on-Digital-Trade.pdf (accessed 25 September 2023).

network latency, to maintain redundancy and resilience for critical data in the wake of physical damage to the storage location.[25]

To establish themselves as reliable recipients of cross-border data, nations must implement rigorous data security laws that mandate data protection standards for both public and private entities, alongside measures for reporting security breaches. Furthermore, governments should consider establishing mutual contractual obligations as a basis for mutual legal assistance and reciprocal transfers of law enforcement data, allowing for the lawful transfer of data. It is important for governments to avoid any attempts to gain unauthorised data access or implement technology backdoors throughout these processes.[26]

Cross-border data-sharing agreements between governments should include mandatory data security measures and an anti-snooping clause, which prohibits governments and connectivity providers from viewing transmitted data across borders except in certain prescribed instances.[27] Additionally, a clear cooperation mechanism between authorities should be established to enhance trust in the data transfer process. These measures may help promote a safe and secure environment for cross-border data transfer while protecting the privacy and security of individuals' data.

2.2.3 Prioritising technical interoperability, data portability and data provenance

Technical interoperability

Technical interoperability pertains to the capacity to exchange data among various systems and empower these systems to effectively utilise the shared data.[28] Technical interoperability can manifest in a syntactic form, necessitating the communication and data exchange among multiple systems, irrespective of variations in programming languages. Alternatively, it may take on a semantic nature, demanding that an individual system comprehends and facilitates the meaningful utilisation of shared data or resources by individuals, organisations and public services.[29]

25 Global Data Alliance 'Cross-border data transfers and data localisation' February 2020, https://globaldataalliance.org/wp-content/uploads/2021/07/02112020GDAcrossborderdata.pdf (accessed 3 March 2023).
26 Global Data Alliance (n 14).
27 World Economic Forum (n 15) 25.
28 A Mittal 'Catalogue of technical standards for digital identification systems' (2022), documents1.worldbank.org/curated/en/707151536126464867/pdf/Catalog-of-Technical-Standards-for-Digital-Identification-Systems.pdf (accessed 25 September 2023).
29 World Economic Forum (n 15) 33.

To ensure that information is accessible and usable in any jurisdiction, systems must possess data interoperability and interconnectivity. This enables data to move seamlessly in the required format to those who require it, when they require it.[30] Practically data is collected and retained by many organisations at global, national and local levels either in an unstructured or structured way. This type of storing and processing of data negates its difficulty to use the data cross-functionally with databases owned by other organisations.[31] Consequently, disseminating or exchanging data among different disconnected applications can pose challenges, given the absence of a standardised format or representation, which complicates its cross-industry utilisation in fields such as artificial intelligence and the internet of things. From our research, we have noted that this can impede cross-border data sharing as data will not be seamlessly transmitted across borders.

The complexity for companies aiming to achieve interoperability and interconnectivity in cross-border data is high, and before transferring data across borders, companies must –

- have a clear understanding of the data protection regulations that apply. This aids companies to understand their obligations under the applicable regime either as a data controller or a data processor.
- conduct a data-mapping exercise to identify and classify the data to be transferred amongst the data collected. Not all data is suitable for cross-border transfers, especially sensitive personal information.
- anonymise or pseudonymise data whenever possible to reduce privacy risks together with using strong encryption methods to protect data during transit and storage. This ensures that even if intercepted, the data remains unreadable to unauthorised parties.
- consider using mechanisms such as standard contractual clauses (SCCs), binding corporate rules (BCRs), or obtaining approval from relevant data protection authorities to legitimise cross-border data transfers.
- assess the necessity of data localisation mandates and the requirement to host data within designated geographic areas to ensure compliance with local data sovereignty regulations.
- enforce rigorous access restrictions and authentication systems to guarantee that only authorised individuals can access and move data; employ role-based access controls (RBAC) to restrict data access to individuals with relevant permissions.
- be transparent with data subjects about the cross-border data transfers, their purpose, and the measures in place to protect their data.
- maintain comprehensive audit trails to track data transfers and access; regularly monitor and review these logs to detect and respond to any unauthorised or suspicious activities.

To attain data interoperability and seamless integration as mentioned above, organisations must fully harness the potential of merging diverse datasets, whether employing fundamental algorithms or artificial intelligence techniques. As this information will be finally harmonised, standardised and stored in

30 United Nations Development Programme (n 11).
31 World Economic Forum (n 15) 35.

structured databases, it will promote data flows to those who need it, where they need it, when they need it, and in the form in which they need it.[32]

Data portability and data provenance

Data portability empowers individuals to move their data between different systems, granting them authority and ownership of their personal data. It also offers a means for users to transition between different service providers.[33] It also provides users with the flexibility to switch between service providers. This issue is particularly important for customers of software as a service (SaaS), who may face challenges when switching services due to data localisation restrictions, which could result in vendor dependency.[34] Vendor entrenchment occurs when pricing models, physical network infrastructure, or unfair contractual clauses create hurdles in transitioning away from a current system, thus obstructing data movement and acting as a barrier to new market entrants. Governments can foster data portability by discouraging vendor entrenchment practices and advocating interoperability standards.

In choosing the best approach to finding the solution to avoid vendor lock-ins, governments can consider either the open standards approach or the open source technologies approach. By adopting an open standards methodology, developers delineate the elements of a system and specify their interactions. This standardisation of system components and communication methods enhances the flexibility and neutrality of systems. In this approach, governments will face reduced risks of becoming bound by exclusive contracts since patents and other proprietary concerns no longer pose obstacles that enable access to raw data and portability. Conversely, the open-source approach involves customers diving into the source code of non-standard parts, rebuilding them, and creating standardised connections. This process may lead to effective solutions but may take years due to design, development and testing.[35]

The significance of data provenance lies in its ability to establish the source of data, its owner, the entities that have processed it, and its complete history from the point of collection, all of which are crucial for safeguarding data authenticity.[36] Blockchain technology has the potential to create a tamper-evident record of data, ensuring that every occurrence of data being transferred or subjected to any form of manipulation can be traced. However, it can prove to be difficult to ascertain the origins of de-identified data or data devoid of historical context. In

32 As above.
33 Organisation for Economic Cooperation and Development 'Mapping approaches to data and data flows report for the G20 Digital Economy Task Force' (2020), http://www.oecd.org/trade/documents/mapping-approaches-todata-and-data-flows.pdf (accessed 25 September 2023).
34 United Nations Development Programme (n 9).
35 ID4Africa ' Putting government back in control Solving vendor lock-in with open standards' 20 June 2019, id4africa.com/2019/almanac/SECURE-IDENTITY-ALLIANCE-SIA.pdf (accessed 20 September 2023).
36 World Economic Forum (n 15) 36.

instances such as these, designating the data as lacking provenance may assist users in evaluating potential risks to data quality when making decisions regarding its appropriate utilisation. Although data provenance is typically viewed as a technical concern, ensuring the accurate attribution of data's origins through proper implementation can elevate data quality during the sharing and transfer of data across geographical boundaries.[37]

2.2.4 Future proofing the policy environment

As the global digital economy continues to expand, the need for cross-border data transfers is becoming increasingly important. However, concerns about data privacy and security have prompted many governments to enact strict regulations around cross-border data sharing. To address these concerns and future proof the policy environment, policy makers must carefully consider the potential risks to and benefits of cross-border data transfers, and develop policies that balance the need for data sharing with the need for data security and privacy. This may include enacting strong data security legislation, implementing mandatory data security measures in cross-border data-sharing agreements, and establishing clear cooperation mechanisms between authorities. By taking a proactive approach to future proofing, the policy environment around cross-border data transfers, governments can help promote a safe and secure environment for data sharing while protecting the privacy and security of individuals' data.

3 Barrier to cross-border data transfers: A spotlight on data localisation

Data localisation pertains to the mandate that data originating from a country's citizens or residents must initially be gathered, handled or stored within the geographical confines of a specific jurisdiction, such as a nation or a regional economic community or union.[38] Some argue that it may be easier to persuade policy makers to recognise the drawbacks of data localisation requirements and convince them to repeal such regulations, rather than attempting to find a common ground for the various data localisation requirements imposed by different jurisdictions.[39] These regulations, despite their intentions to promote data security and privacy, often come with a double-edged sword for businesses. They impose a twofold set of requirements on data processing and storage,

37 F Casalini & J López González 'Trade and cross-border data flows' OECD Trade Policy Papers 220 (2019), https://doi.org/10.1787/18166873 (accessed 17 March 2023).

38 Collaboration on International ICT Policy for East and Southern Africa (CIPESA) "Which way for data localisation in Africa?' (2020), https://cipesa.org/wp-content/files/briefs/Which_Way_for_Data_Localisation_in_Africa___Brief.pdf (accessed 15 March 2023).

39 Hunton & Williams LLP and the United States Chamber of Commerce 'Business without borders: The importance of cross-border data transfers to global prosperity' (2014), https://www.huntonak.com/images/content/3/0/v3/3086/Business-without-Borders.pdf (accessed 15 March 2023).

leading to the inevitable incurrence of additional expenses that otherwise would be avoided if companies had access to the cost-effective and efficient data services hosted in the cloud or international data centres.

The initial form of data localisation arises when governments impose limitations on the cross-border transfer of specific data types. These include personal data; health data; government data; financial data encompassing banking; credit reports; taxation and insurance, along with data associated with user-generated content on internet service platforms; subscriber data; and data held by e-commerce operators. Nations are expanding data localisation requirements by implementing comprehensive regulations that vaguely define the categories of data considered 'sensitive', 'crucial', or pertinent to national security.[40] On the other hand, we have data localisation regulations that require data controllers and data processors to undertake data collection, processing and storage domestically.[41] This not only makes data transfers very complicated, costly and uncertain, but also creates a type of *de facto* localisation where companies have no other option but to store the data locally, especially in the face of massive fines.

Many countries are adopting data-localisation measures due to various reasons, one of which is the desire to exercise greater control over valuable digital assets. While this kind of digital protectionism is a key factor driving these measures, it has been overshadowed by the larger concept of cyber sovereignty, which encompasses the idea of exerting control over digital activities and assets. The significance of data has in recent years experienced a substantial rise, and countries may wish to have this asset closer to them for both psychological and practical reasons. However, simply having data stored locally is not sufficient to create value in and of itself.[42]

Additionally, it is important to highlight that, while data-localisation issues may not be tackled at the local or regional levels, they are, to some extent, being addressed, through international trade agreements such as the Trans-Pacific Partnership (TPP).[43] The TPP provides a test for imposition of data-localisation requirements by signatories with national laws that restrict cross-border transfers. It states that signatories that intend to restrict cross border data flows must satisfy the following:

(1) Is the law necessary to achieve a valid public policy goal?
(2) Is the law free from arbitrary or unjustifiable discrimination in its application?
(3) Does the law avoid being a hidden trade restriction?
(4) Does the law impose information transfer restrictions beyond what is needed to achieve its goal?

40 Cory & Dascoli (n 1) 15.
41 Scharwatt (n 17).
42 Collaboration on International ICT Policy for East and Southern Africa (n 38).
43 UNCTAD (n 21) 14.

The four-part test above may be used as a global test for determining whether data-localisation requirements are excessive.

Restricting data flows has a significant impact on a nation's economy as it measurably reduces the volume of trade, lowers its productivity and increases the prices for small and medium enterprises that are digitally focused and rely on data. Such businesses are an essential growth sector for any country. From a broader private sector perspective, data localisation disincentives the entry of international firms, leading to less competition but, then, foreign companies lack any incentive to invest as they foresee a future where they will incur additional capital and operational expenditure to create local data storage, data centres and other infrastructure.[44] While data-localisation practices are often viewed as a means of protecting citizens' personal data, they may not be effective without robust data protection legislation and a comprehensive approach to controlling data regardless of its physical location.[45] Therefore, we have to ask ourselves whether data localisation requirements are ever justified.

4 Current regulatory framework for cross-border data transfers in Africa

As the digital landscape continues to expand across the African continent, there has been an increasing need to regulate cross-border data transfers. In this part we explore the various regulatory initiatives taking place at the continental, regional and national levels, in a bid to create a robust and secure environment for cross-border data transfer.

4.1 Continental and regional frameworks

4.1.1 African Union

Article 14(6)(a) of the African Union Convention on Cyber Security and Personal Data Protection, 2014 provides that the data controller should not transfer personal data to a non-member state of the AU unless such a state ensures an adequate level of protection of the privacy, freedoms and fundamental rights of persons whose data is being or is likely to be processed. The Convention, however, does not set out what would be considered an adequate level of protection or the factors to be taken into account when assessing the adequacy in the level of protection. Article 14(6)(b) adds that this prohibition is not applicable where

44 United Nations Development Programme (n 9).
45 World Economic Forum (n 15) 23.

the data controller requests authorisation for data transfer from the national data protection authority before transferring any personal data to the third country.[46]

As of 30 September 2023, only 15 countries had ratified the Convention. These are Angola, Cape Verde, Congo, Côte d'Ivoire, Ghana, Guinea, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo and Zambia.[47] The Convention entered into force 30 days after the 15th instrument of ratification had been deposited with the Chairperson of the AU, that is, on 8 June 2023.[48] While a number of countries covered in 4.2 below have data protection laws, most of them are yet to ratify the Convention. This highlights the need for increased efforts to promote and implement the Convention's provisions across the continent. Further, despite the developments across the world in relation to the transfer of personal data, the Convention has not been amended since it was drafted. There is a need for the AU to consider amendments to the Convention as a step towards the harmonisation of standards for the transfer of personal data across the continent.

Section 5.4.5 of the AU Data Policy Framework, 2022 sets out the following recommendations for cross-border data flows, among others: Data-protection frameworks ought to provide minimum standards for cross-border data transfers; the establishment of norms and standards should expressly ensure reciprocity as a central principle for permitting cross-border flows; a degree of capacity must be provided across data-protection agencies to ensure effective cross-border resolution; and AU member states should define a framework and modalities to regulate cross-border data transfers and identify the African entity and persons entitled to manage this system.[49]

Section 5.5.3 of the Framework lists proposed actions in relation to continental instruments. These include that member states should ratify the Malabo Convention and develop additional protocols; to reflect changes since the drafting of the Convention; and to agree on common and harmonious criteria for assessing adequacy in the levels of protection of personal data across the continent to facilitate and enable cross-border transfer of data and to standardise protection.[50]

The digital transformation strategy for Africa highlights policy recommendations and proposed actions. These include support interventions to strengthen cybersecurity at national level such as accelerating the establishment

46 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) art 14.
47 African Union, https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf (accessed 31 March 2023).
48 Malabo Convention (n 46) art 36.
49 African Union, https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf (accessed 31 March 2023).
50 As above.

of personal data protection authorities and making the Malabo Convention consistent with standards such as the modernised Convention 108, the General Data Protection Regulation (GDPR) to promote competitiveness of African companies outside the continent. Support interventions to strengthen cybersecurity at regional and continental level include establishing a framework and mechanism for regional cooperation and mutual assistance and strengthening cooperation between AU bodies and the authorities for the protection of personal data.[51]

4.1.2 Southern African Development Community

The SADC Model Law, 2013 sets out requirements for the transfer of personal data to: a member state that has incorporated the model law into its national laws; a member state that has not incorporated the Model Law into its national laws and to a non-member state. The Model Law permits the transfer of personal data to recipients subject to national law that has been adopted for implementation of the Model Law if the recipient establishes that the transfer of personal data is necessary for the performance of a task carried out in the public interest or subject to the exercise of public body, or if the recipient establishes that it is necessary to transfer the personal data and there is no reason to presume that the data subject's legitimate interests would be prejudiced.[52]

The Model Law also permits the transfer of personal data to recipients other than member states of the SADC that have not incorporated the Model Law Into their national laws on the basis of an adequate level of protection being ensured in the recipient's country, unambiguous consent of the data subject or necessity.[53] The adequacy of the level of protection afforded by the third country shall be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations. The factors that shall be considered include the nature of the data; the purpose and duration of the proposed processing operation(s); the recipient third country; the laws in force in the third country in question and the professional rules and security measures that are complied with in that third country.[54] The transfer of personal data is also permitted where the transfer is made from a register that is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled.[55]

Out of the 16 member states, only five countries, Angola, Mozambique, Mauritius, Namibia and Zambia, have ratified the Malabo Convention. Eleven

51 Digital Transformation Strategy for Africa (2020-2030).
52 Southern African Development Community Model Law (Model Law) 2013 art 43.
53 Model Law arts 44 & 45.
54 Model Law art 44(1)(b).
55 Model Law art 45(1)(f).

countries, Angola, Botswana, Eswatini, Lesotho, Madagascar, Mauritius, Seychelles, South Africa, Tanzania, Zambia and Zimbabwe have enacted data-protection laws. Three countries, Angola, Mauritius and South Africa, have established a data-protection authority.

4.1.3 Economic Community of West African States

Article 36 of the Supplementary Act on Personal Data Protection within the ECOWAS Act, 2010 provides that a data controller shall transfer personal data to a non-member of an ECOWAS country where the country provides an adequate level of protection for privacy, freedoms and the fundamental rights of individuals in relation to the processing or possible processing of such data. The Act, however, does not set out what would be considered an adequate level of protection or the factors to be taken into account when assessing the adequacy in the level of protection. The data controller is required to inform the data protection authority before transferring personal data to a third country.[56]

Out of the 15 member states, only seven countries, namely, Cape Verde, Côte d'Ivoire, Ghana, Guinea, Niger, Senegal and Togo, have ratified the Malabo Convention. Ten countries, Benin, Cape Verde, Côte d'Ivoire, Ghana, Guinea, Mali, Niger, Nigeria, Senegal and Togo, have enacted data-protection laws. Eight countries, Benin, Cape Verde, Côte d'Ivoire, Ghana, Mali, Niger, Nigeria and Senegal, have established a data-protection authority.

4.1.4 East African Community

Recommendation 19 of the Draft EAC Legal Framework for Cyber Laws recommends that further work needs to carried out on the issue of data protection and privacy, to ensure that the privacy of citizens is not eroded through the internet, that legislation providing for access to official information is appropriately taken into account, the institutional implications of such reforms and to take into account fully international best practice in the area.[57]

Out of the seven member states, only Rwanda has ratified the Malabo Convention. Four countries, Kenya, Rwanda, Tanzania and Uganda, have enacted data-protection laws. Three countries, Kenya, Rwanda and Uganda, have established a data-protection authority.

Despite the regional focus of many cross-border data transfer regulations in Africa, the efficacy of such frameworks often hinges on the adequacy of data protection measures in the recipient country, regardless of whether it is a member state of that regional organisation. In practice, this means that countries

56 Supplementary Act on Personal Data Protection within ECOWAS Act, 2010 art 36.
57 Draft EAC Legal Framework for Cyber Laws, 2008.

with robust data-protection safeguards can often bypass regional regulations and facilitate cross-border data transfers more freely than their counterparts without such protections.

4.2 National frameworks

While there are 36 African countries that have enacted data protection laws, we have restricted our review to 17 countries that have official versions of their legislation available in English. Other than the countries highlighted below, Algeria, Angola, Benin, Burkina Faso, Chad, Equatorial Guinea, Egypt, Gabon, Guinea, Madagascar, Mali, Mauritania, Morocco, Niger, Republic of Congo, Senegal, Somalia, Togo and Tunisia, have data-protection laws in place.

4.2.1 Botswana

Section 48 of the Data Protection Act prohibits the transfer of personal data to another country. The Act allows the Minister to designate the transfer of personal data to any country listed in the Order.[58] In 2022 the Minister for State President issued the Transfer of Personal Data Order, pursuant to section 48(2) of the Act, declaring that personal data may be transferred to the 45 countries listed in the order.[59] It is notable that there are only two African countries, South Africa and Kenya; that are included in the Order. The criteria used to determine the countries, however, is unclear.

Despite the restriction in section 48 of the Act, section 49 allows the transfer of personal data on similar bases to those covered in articles 44 and 45 of the SADC Model Law.

4.2.2 Cape Verde

Article 19 of the Data Protection Act provides that the transfer of personal data that are undergoing processing or intended for processing may only take place subject to compliance with the Act and other legislation applicable to issues of personal data protection, and undergoing processing for transfer to another country that has an adequate level of data protection.[60] This adequate level of protection should be assessed in light of all the circumstances surrounding a data transfer or a set of data transfers, in particular, the nature of the data; the purpose and duration of the proposed processing; the country of origin and country of final destination; the rules of law in force in the state in question; and the professional rules and security measures that are complied with in that country.[61]

58 Data Protection Act 32 of 2018 sec 48.
59 Transfer of Personal Data Order, 2022.
60 Data Protection Act Law 133/V/2001 of 22 January (Law 133/V/2001) art 19(2).
61 Law 133/V/2001 (n 60) art 19(3).

The Act permits the transfer of personal data to third countries that do not ensure adequate security safeguards on the basis of unequivocal consent of the data subject, necessity or where the transfer is made from a public register that is intended for information of the public and which is open to consultation either by the general public or by any person who can demonstrate legitimate interest.[62] It is interesting to note that despite the fact that Cape Verde is not an SADC member state, the provisions on transfer of personal data are similar to those covered in articles 44 and 45 of the SADC Model Law.

4.2.3 Côte d'Ivoire

Law 2013-450 provides that a person responsible for the processing can be allowed to transfer personal data to a third country only if the state provides a higher level of protection or equivalent privacy, freedoms and fundamental rights of individuals with regard to the processing which the data are or may be subjected. The person is also required to obtain permission from the protection body before any transfer of personal data.[63] These provisions are similar to those in the Supplementary Act on Personal Data Protection within ECOWAS Act, 2010.

4.2.4 Eswatini

The provisions on cross-border transfer of personal data outside Eswatini under the Data Protection Act are similar to articles 43, 44 and 45 of the SADC Model Law.[64] The Act provides for transfer of personal information within SADC and non-SADC member states.

4.2.5 Ghana

While Ghana has a data protection law, the Data Protection Act contains no provisions on cross-border transfer of personal data.

4.2.6 Kenya

The Data Protection (General) Regulations require a data controller or data processor who is transferring personal data to a country outside Kenya to ascertain that the transfer is based on appropriate data protection safeguards, an adequacy decision made by the data commissioner, necessity or consent of the data subject.[65] A transfer of personal data is based on the existence of appropriate

62 Law 133/V/2001 (n 60) art 20.
63 Law 2013-450 dated June 19 2013 art 26.
64 Data Protection Act 5 of 2022 secs 32 & 33.
65 Data Protection (General) Regulations 2021 (General Regulations) reg 40.

safeguards where a legal instrument containing appropriate safeguards for the protection of personal data binding the intended recipient that is essentially equivalent to the protection under the Act and these Regulations or the data controller, having assessed all the circumstances surrounding transfers of that type of personal data to another country or relevant international organisation, concludes that appropriate safeguards exist to protect the data.[66]

A country is also deemed to have appropriate safeguards if it has ratified the Malabo Convention, a reciprocal data protection agreement with Kenya or a contractual binding corporate rules among a concerned group of undertakings or enterprises.[67] The first basis currently is questionable as Kenya is yet to sign and ratify the Malabo Convention.

4.2.7 Lesotho

The Data Protection Act imposes limitations on the transfer of personal data to a foreign third party. The recipient must be subject to a law, code of conduct or contract that effectively upholds principles for reasonable processing of the information that are substantially similar to the information protection principles under the Act, and includes provisions that are substantially similar to those relating to further transfer of personal information from the recipient to third parties in foreign countries.[68] The Act also permits the transfer of personal data on the basis of consent of the data subject or necessity.[69] The Act also has a very unique basis for transfer, where the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer or, if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.[70]

4.2.8 Mauritius

The Data Protection Act allows a data controller or data processor to transfer personal data to another country on the basis of providing to the commissioner proof of appropriate safeguards, the data subject's explicit consent to the proposed transfer, necessity or the transfer being made from a register that, according to law, is intended to provide information to the public and which is open for consultation by the public or by any person who can demonstrate a legitimate interest.[71]

66 General Regulations (n 65) reg 41(1).
67 General Regulations (n 65) reg 42.
68 Data Protection Act 5 of 2011 sec 52.
69 As above.
70 As above.
71 Data Protection Act 20/2017 sec 36.

4.2.9 Nigeria

The Nigeria Data Protection Regulation permits the transfer of personal data to a foreign country or an international organisation where the National Information Technology Development Agency has decided that the foreign country, territory or one or more specified sectors within that foreign country, or the international organisation in question ensures an adequate level of protection.[72] The Attorney-General of the Federation (HAGF) is required to take into consideration the legal system of the foreign country particularly in the areas of rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including public security, defence, national security and criminal law and the access of public authorities to personal data.[73]

Where the National Information Technology Development Agency or the HAGF has not issued a decision as to the adequacy of safeguards in a foreign country, a transfer or a set of transfers of personal data to a foreign country or an international organisation shall take place on one of the bases specified in the Regulation, that is, explicit consent of the data subject or necessity.[74] Nigeria recently enacted the Data Protection Act that contains additional provisions on transfer of personal data. The bases provided in the Act are similar to those in GDPR which are covered in part 5 below, that is, the recipient is subject to law on personal data, there are binding corporate rulers, contractual clauses, code of conduct or a certification mechanism that provides an adequate level of data protection that is similar to the Act.

4.2.10 Rwanda

The transfer of personal data to a third party outside Rwanda is permitted under the law relating to the Protection of Personal and Privacy if a data controller or data processor has obtained authorisation from the supervisory authority after providing proof of appropriate safeguards with respect to the protection of personal data, on the basis of consent of the data subject or necessity.[75]

4.2.11 São Tomé and Príncipe

Article 19 of the Law on Protection of Personal Data provides that the transfer of personal data to a place outside the national territory may only be carried out in compliance with the provisions of this law and if the legal order to which they are transferred ensures a suitable level of protection.[76] This adequate level of

72 Nigeria Data Protection Regulation 2019 (NDPR) part 2.11.
73 As above.
74 NDPR (n 72) part 2.12.
75 Law 058/2021 of 13 October 2021 relating to the protection of personal data and privacy art 48.
76 Law 03/2016 Protection of Personal Data (Law 03/2016) art 19(1).

protection should be assessed in light of all the circumstances surrounding a data transfer or a set of data transfers, taking into account, in particular, the nature of the data, the purpose and the duration of the processing or planned treatments, the countries of origin and of final destination, the general or special rules of law in force in the legal system concerned, as well as the professional rules and security measures that are respected in that same order.[77]

The Law also permits the transfer of personal data to third countries that do not ensure an adequate level of protection on the basis of unequivocal consent of the data subject, necessity or where the transfer is carried out on the basis of a public register that, according to the law or administrative regulation, is intended to inform the public and is open to consultation with the general public or any person who can prove a legitimate interest.[78]

4.2.12 Seychelles

The Data Protection Act takes a unique approach to the issue of the transfer of personal data where, instead of providing the grounds on which transfers would be permissible, it provides for a transfer prohibition notice. The Act provides that if it appears to the commissioner that a person registered as a data user or as a data user who also carries on a computer bureau proposes to transfer personal data held by him to a place outside the Seychelles, the commissioner may, if satisfied that the transfer is likely to contravene or lead to a contravention of any data protection principle, serve that person with a transfer prohibition notice prohibiting him from transferring the data either absolutely or until he has taken such steps as are specified in the notice for protecting the interests of the data subjects in question.[79]

The Act, however, is yet to come into operation, and on 16 March 2023 the Data Protection Bill which seeks to repeal the Act was published. The Bill has taken a unique approach by providing for conditions in which sensitive personal data may be transferred outside Seychelles. For transfer of personal data, this is subject to the recipient country being part of a cross-border privacy rules system that ensures that the system's standards are enforceable against the data controllers and data processors as part of the certification system and data controllers and data processors have implemented security measures using a risk-based approach.[80] This is a different approach to that taken by other African states given that there currently is no certification system in place and there is no reference made to recipient countries having an adequate level of data protection.

77 Law 03/2016 (n 76) art 19(2).
78 Law 03/2016 (n 76) art 20.
79 Data Protection Act 9 of 2003 sec 16.
80 Data Protection Bill 2023 clause 48(3).

4.2.13 South Africa

The Protection of Personal Information Act (POPIA) restricts the transfer of personal data to a third party who is in a foreign country unless the recipient of the information is subject to a law, binding corporate rules or binding agreement. The requirements should provide an adequate level of protection that effectively upholds the principles for reasonable processing of the information that are substantially similar to the information protection principles under the Act, and includes provisions that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person and includes provisions substantially similar to the provision relating to the further transfer of personal information from the recipient to third parties who are in a foreign country. [81]

The Act also permits the transfer of personal data on the basis of consent of the data subject or necessity.[82] The Act, similar to the Lesotho Data Protection Act, permits a data controller or data processor to transfer personal data, where the transfer is for the benefit of the data subject and it is not reasonably practicable to obtain the consent of the data subject to that transfer and, if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.[83]

4.2.14 Tanzania

The provisions on cross-border transfer of personal data outside Tanzania under the Personal Data Protection Act are similar to articles 43, 44 and 45 of the SADC Model Law. The Act provides for the transfer of personal data to states with and without a legal framework providing for adequate data protection. Tanzania also passed the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 that provide for the procedure and requirements for applications for transfer of personal data.

4.2.15 Uganda

The Data Protection and Privacy Act provides that where a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller shall ensure that the country in which the data is processed or stored has adequate measures in place for the protection of personal data at the least equivalent to the protection provided by this Act or the data subject has consented.[84]

81 Protection of Personal Information Act 4 of 2013 sec 72.
82 As above.
83 As above.
84 Data Protection and Privacy Act 9 of 2019 sec 19.

The Data Protection and Privacy Regulations expound on this provision, highlighting that the data controller or data processor is required to provide proof of the adequate measures or the data subject's consent to the Personal Data Protection Office.[85] For purposes of transfer on the basis of the existence of adequate measures for protection of personal data, the office is required to publish a notice in the *Gazette* specifying the countries that have adequate measures in place for the protection of the personal data at least equivalent to the protection required by the Act.[86] It is only where a country does not appear on the list that the data controller or data processor will be required that the country has adequate measures in place.[87]

4.2.16 Zambia

The Data Protection Act provides that a data controller shall process and store personal data on a server or data centre located in Zambia. The Minister, however, may prescribe categories of personal data that may be stored outside Zambia.[88] Personal data other than data that is categorised in accordance with the above provision may be transferred outside the country where the data subject has consented, and the transfer is made subject to standard contracts or intra group schemes that have been approved by the Data Protection Commissioner; or the Minister, has prescribed that transfer outside the country is permissible; or the Data Protection Commissioner approves a particular transfer or set of transfers as permissible due to a situation of necessity.[89]

4.2.17 Zimbabwe

The Data Protection Act allows the transfer of personal data only where the country of the recipient ensures an adequate level of protection and the data is transferred solely to allow tasks covered by the competence of the controller to be carried out.[90]

The adequacy of the level of protection afforded by the third country shall be assessed in light of all the circumstances surrounding a data transfer operation or set of data transfer operations with particular consideration being given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the recipient third country, the laws relating to data protection in force in the third country in question and the professional rules and security measures that are complied with in that third country.[91]

85 Data Protection and Privacy Regulations 2021 reg 30(1).
86 Data Protection and Privacy Regulations (n 85) reg 30(4),
87 Data Protection and Privacy Regulations (n 85) reg 30(5).
88 Data Protection Act 3 of 2021 sec 70.
89 Data Protection Act (n 88) sec 71.
90 Data Protection Act 5/2021 sec 28.
91 As above.

The Act permits the transfer of personal data to third countries that do not ensure an adequate level of protection on the basis of unambiguous consent of the data subject, necessity or where the transfer is made from a public register that, according to acts or regulations, 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 legitimate interest.[92]

From the above review of the legislative frameworks in place in various African countries, it is clear that there are varied approaches to cross-border transfer. Most countries have taken the approach of adopting the provisions in regional instruments in the regional organisations of which they are members. The basis that is captured in most legal instruments is countries having in place an adequate level of protection to personal data. However, there are some countries that do not provide the factors to be considered in determining this and whether the data protection authorities will issue adequacy decisions to ensure that the data controllers and data processors are not required to assess the level of adequacy. Further, while having data protection laws in place is a step in the right direction, it is possible for the varying conditions to be considered as less of an aid and more of a limitation to cross-border transfer of personal data.

5 Approaches taken by other regions in regulation of cross-border data transfers

We now review approaches taken by other regions in the regulation of cross-border data transfers, with a focus on the European Union (EU) and the Asia-Pacific Economic Cooperation (APEC).

5.1 European Union

Chapter V of the EU General Data Protection Regulation (GDPR) provides for transfers of personal data to third countries or international organisations. The general principle for transfers is that any transfer of personal data that is undergoing or is intended for processing after transfer to a third country or an international organisation shall take place only if, subject to the other provisions of GDPR, the conditions laid down in chapter V are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.[93]

GDPR sets out two general bases for the transfer of personal data, namely, an adequacy decision or appropriate safeguards. A transfer of personal data to a third

92 Data Protection Act (n 90) sec 29.
93 General Data Protection Regulations 2016/679 (GDPR) art 44.

country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.[94] The Commission so far has recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the UK GDPR and the Law Enforcement Directive, and Uruguay as providing adequate protection.[95]

GDPR also permits, in the absence of an adequacy decision, the transfers of personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[96] There are two categories of transfers subject to appropriate safeguards, namely, (i) appropriate safeguards without authorisation from a supervisory authority; and (ii) appropriate safeguards with authorisation from a supervisory authority.

The appropriate safeguards may be provided for, without requiring any specific authorisation from a supervisory authority, by a legally-binding and enforceable instrument between public authorities or bodies; binding corporate rules; standard data protection clauses adopted by the Commission; standard data protection clauses adopted by a supervisory authority and approved by the Commission; an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.[97]

Where authorisation from a supervisory authority is required for the transfer of personal data, the appropriate safeguards may be provided for in contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation or provisions that are inserted into administrative arrangements between public authorities or bodies, including enforceable and effective data subject rights.[98]

GDPR also provides that in the absence of an adequacy decision or appropriate safeguards, personal data may be transferred to a third country or international

94 GDPR (n 93) art 45.
95 European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (accessed 31 March 2023).
96 GDPR (n 93) art 46.
97 As above.
98 As above.

organisation on the basis of a data subject's explicit consent, necessity or where the transfer is made from a register which according to EU 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 prove a legitimate interest.[99]

The European Data Protection Board (EDPB), which is established under article 68 of GDPR, has issued various guidelines and recommendations on the transfer of personal data pursuant to its powers under article 70 of GDPR. These include:

- Guidelines 2/2018 on derogations of article 49 under Regulation 2016/679: These guidelines provide guidance on the application of article 49 of GDPR on derogations for transfer of personal data to third countries.[100]
- Guidelines 2/2020 on articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies: The guidelines set out the expectations of the EDPB on the safeguards required to be put in place by a legally-binding and enforceable instrument between public bodies or by provisions to be inserted into administrative arrangements between public bodies.[101]
- Guidelines 04/2021 on Codes of Conduct as tools for transfers: The guidelines specify the application of article 40(3) of GDPR relating to codes of conduct as appropriate safeguards for transfers of personal data in line with article 46(2)(e) of GDPR.[102]
- Guidelines 05/2021 on the interplay between the application of article 3 and the provisions on international transfers as per chapter V of GDPR: The purpose of the guidelines is to assist data controllers and processors with identifying whether a processing operation constitutes a transfer to a third country or to an international organization, and whether they would therefore have to comply with the provisions of chapter V of GDPR.[103]
- Guidelines 07/2022 on certification as a tool for transfers: These guidelines provide practical guidance on the application of article 46(2)(f) of GDPR on transfers of personal data to third countries or to international organisations on the basis of certification.[104]
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: The EDPB adopted the recommendations to help data exporters with the task of

99 GDPR (n 93) art 49.
100 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (accessed 31 March 2023).
101 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202002_art46guidelines_internationaltransferspublicbodies_v2_en.pdf (accessed 31 March 2023).
102 https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf (accessed 31 March 2023).
103 https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf (accessed 31 March 2023).
104 https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_en_0.pdf (accessed 31 March 2023).

assessing third countries and identifying appropriate supplementary measures for protection of personal data.[105]

- Recommendations 1/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding Corporate Rules (art 47 of GDPR): These recommendations are meant to, among other things, provide a standard form for the application for approval of binding corporate rules for controllers.[106]

One of the critiques of the adequacy decision approach provided for in GDPR is that it may be difficult to find the required adequacy for cross-border data transfer which proposes the inevitable doubts over the effectiveness and suitability of adequacy decision as an instrument to authorise such data transfer.[107] Another critique is that the approach presents developing countries with a dilemma where, if they seek an adequacy decision, they should have enacted a national data protection law that is in essence, equivalent to that of the EU.[108]

5.2 APEC

The APEC Privacy Framework provides guidance to member economies on the implementation of the Framework, stating that they should have regard to the following basic concept in considering the adoption of measures designed for domestic implementation of the APEC Privacy Framework: Personal data should be processed in a way that protects data subjects' privacy and allows the data subjects and economies to maximise the benefits of data flows within and across borders and that, consequently, as part of establishing or reviewing their privacy protections, member economies should take all reasonable and appropriate steps to identify and remove unnecessary barriers to data flows and avoid the creation of any such barriers.[109]

With regard to cross-border privacy mechanisms, the Framework states that member economies have developed the Cross-Border Privacy Rules (CBPR) system, which provides a practical mechanism for participating economies to implement the APEC Privacy Framework in a cross-border context, and to provide a means for organisations to transfer personal data across borders in a

105 https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (accessed 31 March 2023).

106 https://edpb.europa.eu/system/files/2022-11/edpb_recommendations_20221_bcr-c_referentialapplicationform_en.pdf (accessed 31 March 2023).

107 S Chen 'Cross-border data transfer after Schrems II: The globalisation of EU standards of data protection through adequacy decisions or trade agreements?' Lund University, https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9050792&fileOId=9050794 (accessed 30 September 2023).

108 C Gay 'The GDPR's effect on transatlantic relations' University of Chicago Law School, The GDPR's Effect on Transatlantic Relations (uchicago.edu) (accessed 30 September 2023).

109 https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 (accessed 31 March 2023).

manner in which individuals may trust that the privacy of their personal data is protected.[110]

The APEC Cross Border Privacy Rules system, endorsed by APEC leaders in 2011, is a voluntary accountability-based scheme to facilitate privacy respecting personal information flows among APEC economies.[111] There currently are nine participating economies in the CBPR system: Australia, Canada, Mexico, Japan, the Republic of Korea, the Philippines, Singapore, Chinese Taipei, and the United States of America.[112]

On cross-border transfer, the Framework states that a member economy should refrain from restricting cross-border flows of personal data between itself and another member economy where the other economy has in place legislative or regulatory instruments that give effect to the Framework or sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures (such as the CBPR) put in place by the personal information controller to ensure a continuing level of protection consistent with the Framework and the laws or policies that implement it. Further, any restrictions to cross-border flows of personal data should be proportionate to the risks presented by the transfer, taking into account the sensitivity of the information, and the purpose and context of the cross-border transfer.[113]

Some of the limitations identified in relation to the APEC CBPR system include that it is voluntary and, therefore, non-binding, and that there is a lack of clarity in what the system will achieve given that it does not supersede national data protection laws.[114]

6 A case for the continental cooperation in the harmonisation of a regional legal framework for cross-border data transfers in Africa

One of the main obstacles to cross-border data transfers in Africa is the fragmented and divergent national mandates concerning the collecting and processing of personal data. The presence of multiple data protection regulations that are applicable may lead to ambiguity for governments, businesses and individuals,

110 https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 (accessed 31 March 2023).
111 http://cbprs.org/about-cbprs/ (accessed 31 March 2023).
112 http://cbprs.org/government/ (accessed 31 March 2023).
113 https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1 (accessed 31 March 2023).
114 https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (accessed 30 September 2023).

making it unclear which rules pertain to a particular cross-border data transfer.[115] More specifically, certain nations implement local storage requirements (referred to as data sovereignty or data protectionism) with the specific aim of compelling data to be stored and retained within their borders. In Botswana, only two African countries have received approval for transferring personal data, and in Côte d'Ivoire, regulations for cross-border data transfers mandate that the recipient country must ensure a level of protection that is equal to or greater than that of the originating country.

Further, while most countries, such as Botswana, Cape Verde, Eswatini, Nigeria, São Tomé and Príncipe, South Africa, Uganda and Zimbabwe, provide for transfer of personal data on the basis of adequate level of protection in the recipient country, and some even go a step further to set out the factors that should be considered in determining this adequacy. It is unclear what would qualify as adequate. It is possible that some jurisdiction may not require a high level of compliance, which may lead to difficulties in determining what is adequate. As such, it is imperative for African nations to collaborate in establishing standardised criteria for evaluating sufficient levels of protection.

A number of nations also permit jurisdictional personal data flows if an organisation has put up appropriate security measures, but does not expound on what would amount to appropriate safeguards. Kenya allows for cross-border data transfers if appropriate safeguards are in place. Such safeguards can come in the form of an agreement binding the recipient of data, providing protection for personal data equivalent to that provided by the Kenyan Data Protection Act and Regulations. Alternatively, a transfer may be allowed if the data controller has concluded that appropriate safeguards exist to protect the data. The Regulations, however, do not provide a format of the binding instrument, contrary to the EU approach that provides template standard contractual clauses. It is necessary for African countries to have a harmonised framework in place that would assist in the determination of what would constitute appropriate safeguards.

The growing amounts of data being transferred across borders in Africa underscore the necessity for a flexible and unified system that can handle both current and future data exchanges. This system should take into account variations in local laws, acknowledge commonalities among local regulations, safeguard individual rights, and ensure effective enforcement in case of any breaches. Hence, to promote collaboration among African nations on protecting personal data, it is essential to consider various avenues. These include establishing regional cross-border data frameworks with adequacy assessments; implementing a safe harbour framework; and incorporating suitable data protection measures.

115 Organisation for Economic Cooperation and Development (n 33) 30.

Under the white list or adequacy decisions approach, each country creates a white list of approved countries with adequate data protection measures, and requires that cross-border data transfers be covered by protective contracts. By setting a common standard for data protection, this approach can facilitate the harmonisation of privacy laws across the continent and promote bilateral trade negotiations. Ultimately, achieving a degree of commonality in data protection principles is key to enabling smooth cross-jurisdictional data transfers between jurisdictions with differing data protection laws. The harmonisation of data protection rules on cross-border transfer of data starts from the local and the regional context. This means that locally African countries must borrow and apply certain applicable concepts and guidelines contained in other international regional frameworks.[116] Given this effort, it is essential that there be greater convergence between the specific ways in which countries approach the regulation of data transfers.

On the contrary, the safe harbour framework, originally developed through negotiations between the United States of America and the European Commission, aims to establish an efficient mechanism for businesses operating in a region with limited data protection regulations to transfer data to another jurisdiction with more robust data protection rules and safeguards in place. In Africa, a possible implementation could involve companies seeking safe harbour certification by aligning their privacy practices with the safe harbour privacy principles, as determined by the AU. They would then be required to submit a self-certification form to the relevant regional authority, which may be the AU or a regional bloc. Additionally, companies would need to make their safe harbour privacy policy accessible to the public, clearly demonstrating their commitment to complying with the privacy principles.[117]

Moreover, as the AfCFTA continues to gain momentum and evolve as a central pillar of the continent's economic landscape, it not only is prudent but also imperative to recognise and proactively tackle the intricate issue of cross-jurisdictional data transfers arising from trade agreements. Incorporating provisions pertaining to cross-border data transfers into trade agreements is not a novel concept but rather an essential and forward-looking strategy. By doing so, African nations can harness the synergistic potential that exists at the intersection of digital commerce and cross-border trade. This approach ensures that the benefits of AfCFTA extend seamlessly into the digital realm, fostering an environment conducive to innovation, efficiency and economic growth.

Acknowledging and addressing cross-border data transfers within trade agreements also underscores Africa's commitment to embracing the opportunities presented by the digital age. It reinforces the continent's resolve to

116 United Nations Development Programme (n 9).
117 Hunton & Williams (n 39).

be at the forefront of shaping the future of global trade, where data flows play an increasingly pivotal role. By proactively integrating data transfer considerations into trade accords, African nations demonstrate their readiness to engage in the global digital economy on equal terms, fostering an environment of trust and collaboration with international partners.

7 Conclusion

In conclusion, Africa finds itself at a pivotal juncture on its transformative path into the digital age, with cross-border data transfers serving as a linchpin of this profound journey. The unimpeded circulation of data across borders possesses the extraordinary potential to unlock unparalleled economic prospects and usher in new horizons for businesses and visionary entrepreneurs across the continent. Nonetheless, the absence of a harmonised legal framework for governing these data transfers has cast formidable hurdles and stymied the digital economy's expansion within Africa.

It is imperative that the AU assumes a leading role in the formulation of a comprehensive continental legal framework – one that deftly balances the imperatives of data protection and privacy with the boundless opportunities afforded by an unrestrained digital economy. The economic growth prospects are monumental should African nations unite in harnessing the advantages of cross-border data transfers. To surmount these challenges, seamless cooperation between African governments and regional entities becomes a pressing necessity, with the aim of establishing a uniform legal framework for these data transfers. This framework should be meticulously calibrated to safeguard data integrity and privacy, while concurrently reaping the dividends of an unbridled digital economy. By doing so, Africa can fully harness the potential of its burgeoning digital economy, thus sculpting a prosperous future for its citizens.

In the swiftly-evolving digital landscape, time stands as an unforgiving arbiter. African nations must act expeditiously in orchestrating a harmonised legal framework for cross-border data transfers, positioning themselves as trailblazers in the global digital arena. Failing to do so carries the perilous risk of relegating Africa to a backseat in the digital era, forfeiting the colossal economic and societal advantages inherent in digital transformation. As a renowned data analyst astutely noted, 'data is like the air we breathe. We don't think about it until it's not there.' Much like clean air is indispensable for human survival, the uninterrupted flow of data within a harmonised framework is imperative for Africa's economic prosperity and all-encompassing development.

African Journal on Privacy & Data Protection

To cite: B Mutiro & O Saki 'The Cyber and Data Protection Act of Zimbabwe: A critical analysis' (2024) 1 *African Journal on Privacy & Data Protection* 50-80
https://doi.org/10.29053/ajpdp.v1i1.0004

The Cyber and Data Protection Act of Zimbabwe: A critical analysis

*Blessing Mutiro**
Early-Stage Researcher, Castlebridge, Dublin; PhD Researcher, Trinity College, Dublin, Ireland

*Otto Saki***
Doctoral candidate, University of the Western Cape, South Africa

Abstract:

The Cyber and Data Protection Act of Zimbabwe is the first comprehensive data protection statute covering both the public and private sectors and setting up a data protection authority. Its provisions are vital to the protection of the fundamental human right to privacy. This is in the context of the government prioritising cybersecurity over privacy, with the private sector being complicit. This context of cybersecurity over privacy is seen through the government's intention in passing the Act of which the provisions focus more on cybersecurity rather than on data protection. Against this background, this study evaluates the Cyber and Data Protection Act to establish whether its provisions are adequate to protect and ensure privacy and data protection despite the cybersecurity

* LLBS (University of Zimbabwe) LLM (University of Birmingham) blessing.mutiro@castlebridge.ie/mutirob@tcd.ie. The author has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie Grant Agreement 813497.

** LLBS (University of Zimbabwe) LLM (Columbia University) LLM (Open University Tanzania); otto.saki@caa.columbia.edu. The authors acknowledge the editorial support and attention to detail that Mr Mduduzi Ruwitah provided in preparing this article. The authors are grateful to the two anonymous reviewers for their comments. All errors are those of the authors.

intention and focus. The study examines the Zimbabwean data protection regime from a customary law, common law and international law perspective, comparing the Act against European Union-style legislation that has inspired and is the bedrock of the Act. This is a study of what has been enacted, and what may have been enacted in Zimbabwe.

Key words: data privacy; data protection; personal information; cybersecurity

1 Introduction

On 3 December 2021 the Cyber and Data Protection Act (CDPA)[1] of Zimbabwe became law.[2] The object of the Act is 'to increase cyber security in order to build confidence and trust in the secure use of information and communication technologies by data controllers, their representatives and data subjects'.[3] Before the CDPA, there was no Zimbabwean law governing data protection following the repeal of the Access to Information and Protection of Privacy Act (AIPPA)[4] that only applied to public entities. A literal reading of the CDPA objectives indicates the government's intent to invest in cybersecurity, not data protection. CDPA comes at a time when there has been misuse of personal data by public and private entities.[5] Concurrently, the government has increased surveillance on citizens using artificial intelligence.[6]

The CDPA enactment benefits from the global and continental discussions on data protection spurred by developments in the European Union (EU) through the General Data Protection Regulation (GDPR) and the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention). The GDPR is viewed as having considerably influenced African data protection frameworks, with disastrous impact.[7] The Malabo Convention, which entered in force on 8 June 2023, attempts to frame an African approach

1 CDPA [Chapter 11:12] 5 of 2021.
2 Before it was gazetted as law, the short title of the Act was Cyber Security and Data Protection Bill. Several changes were made by legislators and the minister responsible for the Bill. These changes are to be found at http://www.veritaszim.net/node/4863 (accessed 6 December 2021).
3 CDPA (n 1) sec 2.
4 Access to Information and Protection of Privacy Act (AIPPA) [Chapter 10:27] Act 5 of 2003.
5 Media Institute of Southern Africa 'Zimbabwe's urgent need for data privacy laws' 13 July 2018, http://zimbabwe.misa.org/2018/07/13/zimbabwes-urgent-need-data-privacy-laws/ (accessed 27 March 2023). One such incident was during the 2018 elections when voters received messages that urged them to vote for a specific Zimbabwe African National Union – Patriotic Front (ZANU PF) Member of Parliament specific to their constituency and to vote for the ZANU PF presidential candidate. It was most likely that the information had been obtained from the voters' roll and subsequently used to target voters. However, there was no way in which one could compel ZANU PF to disclose from where they had obtained the information and, as such the scandal simply faded and everyone forgot about it.
6 G Maunganidze 'Letter to Speaker of National Assembly: Increase in collection of personal data in the absence of adequate data privacy legislation' 4 December 2018, http://zimbabwe.misa.org/2018/12/04/letter-to-speaker-of-national-assembly-increase-in-collection-of-personal-information-in-the-absence-of-adequate-data-privacy-legislation/ (accessed 27 March 2023).
7 C Mannion 'Data imperialism: The GDPR's disastrous impact on Africa's e-commerce markets' (2021) 53 *Vanderbilt Journal of Transnational Law* 685.

to data protection, albeit with limitations.[8] In addition, the Council for Europe has modernised Convention 108 on data processing (Convention 108+),[9] which is open to non-European countries for membership. Zimbabwe has not been invited to accede to Convention 108+ and has not ratified the Malabo Convention. Several judicial and legislative developments also affect data protection. Considering these developments, this article continues by studying the resonance of CDPA with African multinational data protection agreements and international standards. It also provides a critical analysis of general protections of personal data in Zimbabwe.

Through a doctrinal assessment of the main features and provisions of the CDPA, the article focuses on what has been enacted and what may have been enacted. The article also discusses data protection under common and customary law. It then discusses international privacy and data protection standards and commitments. This is followed by a historical background to data protection in Zimbabwe. An overview and discussion of the obligations, main components, and rights in CDPA follows. The discussion is alongside a critique of CDPA, and recommendations to improve the Act's utility in the protection of personal information.[10]

2 Data protection under common law and customary law

Zimbabwe has a dual legal system of general law consisting of common law and statute, and African customary law.[11] According to section 192 of the Constitution of Zimbabwe, the law to be administered by the courts is the law in force on the 'effective date',[12] being the date on which the Constitution became law.[13] According to section 89 of the Constitution,[14] the applicable law is the 'law in force in the Colony of the Cape of Good Hope on 10 June 1891, as modified by subsequent legislation having in Zimbabwe the force of law'.[15] The law applicable at the Cape of Good Hope on 10 June 1891 was Roman-Dutch law with English law grafting.

The right to protection of personal data is novel. There is no common law right to data protection within Roman-Dutch law. A right to privacy, however, exists.

8 G Greenleaf & B Cottier 'International and regional commitments in African data privacy laws: A comparative analysis' (2022) 44 *Computer Law and Security Review* 105638.
9 Council of Europe Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data 2018 (Convention 108+).
10 It does not cover consequential amendments to the Criminal Law Codification and Reform Act [Chapter 9:23], the Criminal Procedure and Evidence Act [Chapter 9:07] and the Interception of Communications Act [Chapter 11:20].
11 L Madhuku *An introduction to Zimbabwean Law* (2010).
12 Constitution of Zimbabwe Act 20 of 2013, sec 332.
13 As above.
14 Constitution of Zimbabwe Act, 2008. The Act, which was the 19th Amendment to the Constitution entered into force on 13 February 2009 and amended the Constitution of Zimbabwe. It was repealed and amended by the Constitution of Zimbabwe Act 20 of 2013.
15 Constitution of Zimbabwe (n 12) sec 89.

Zimbabwe's common law right to privacy derives from the common law of South Africa.[16] It is worth considering whether the common law right to privacy applies to data protection given the overlap between the right to private life, a pillar of the right to privacy, and the right to protection of personal data.[17] A claim for a right to privacy under common law is related to personality.[18] When the right to privacy is violated, there are four main remedies,[19] namely, the *actio iniuriarum*, which is the recovery of sentimental damages or satisfaction for injured feelings; the *actio legis Acquiliae*, where the plaintiff has suffered monetary loss; an interdict where there is impending or continuous infringement;[20] and a retraction coupled with an apology.[21] The applicability of the common law right of privacy to data protection is questionable. Ncube argues that the active control principles of data protection differ from common law privacy protections, making common law privacy protections inadequate for purposes of data protection.[22] Further, for a common law right to privacy to apply to data protection, a two-point process must be undertaken. The first is full utilisation of the common law, and the second is an individual controlling the data. If the individual is not in control of the data, it is unlikely that the common law right to privacy applies. Examples of where the common law right to privacy would apply to data protection are where photographs are taken[23] and telephones are tapped without the subject's consent.[24] In these examples, Zimbabwean courts can extend the common law right to privacy to data protection. However, they have been reluctant to give the common law right to privacy an expansive interpretation.[25] Although *Nsoro*[26] shows a shift towards an expansive interpretation as the Court held that society ought to respect privacy of communications,[27] it is unlikely that a common law right to privacy applies to data protection.

The concept of data protection in Zimbabwe was first introduced by AIPPA and, subsequently, the CDPA. There is no prior Zimbabwean case law on customary law and on data protection. Similarly, the existence of a right to privacy in Zimbabwe's customary law is doubtful as privacy is an abstract concept in traditional African societies.[28] An individual's personhood is intricately linked

16 C Ncube 'A comparative analysis of Zimbabwean and South African data protection systems' (2004) 1 *Journal of Information, Law and Technology* 1.
17 M Gracia Porcedda 'The recrudescence of security v privacy after the 2015 terrorist attacks and the value of "privacy rights" in the European Union' in E Orrù, M Grazia Porcedda & S Weydner-Volkmann *Rethinking surveillance and control. Beyond the 'security vs privacy' debate* (2017) 149.
18 *S v A & Another* 1971 (2) SA 476 (C) 297.
19 Ncube (n 16) 107.
20 *Rhodesian Printing & Publishing v Duggan* 1975 (1) SA 590 (A).
21 *Mineworkers Investment Co (Pty) Ltd v Modibane* 2002 (6) SA 512.
22 *Rhodesian Printing & Publishing v Duggan* (n 20).
23 *La Grange v Schoeman* 1980 (1) SA 885.The Court held that taking photographs without consent of the person constituted an invasion of the right to privacy.
24 *Reid v Daly v Hickman & Others* 1980 ZLR 540 (A).
25 *Mr & Mrs X v Rhodesia Printing & Publishing Co Ltd* 1974 (4) SA 508 (R).
26 *S v Nsoro* HH 190-16 (unreported).
27 As above.
28 AB Makulilo 'Protection of personal data in sub-Sahara Africa' doctoral thesis, University of Bremen, 2012 277; EM Bakibinga 'Managing electronic privacy in the telecommunications

with their community, as aptly defined by concepts such as ubuntu.[29] *The identity of the individual is based on them being a member of the community, which is the custodian of the individual's rights*.[30] It thus is difficult for an individualistic right to privacy to thrive. The communitarian environment, however, provides a framework for relational or group privacy.[31] It therefore is unlikely that there exists an African customary law right to privacy useable to assert personal data protection.

3 International privacy and data protection standards and commitments

Zimbabwe's international privacy commitments stem mainly from the Universal Declaration of Human Rights (Universal Declaration)[32] and the International Covenant on Civil and Political Rights (ICCPR).[33] The right to privacy is also to be found in article 10 of the African Charter on the Rights and Welfare of the Child (African Children's Charter).[34] These instruments inspired the right to privacy in most African countries under post-independence constitutions.[35] Zimbabwe's first post-independence Constitution, however, lacked an explicit right to privacy.[36]

African data protection standards have been influenced by developments in the EU.[37] These include the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108)[38] and the Data Protection Directive.[39] Convention 108 allows non-Council of Europe members to accede to it. Some African countries have ratified the Convention and its additional protocol.[40] The Convention was recently modernised into Convention 108+. Zimbabwe has neither signed nor ratified either convention. Data protection standards of Convention 108, the additional

sub-sector: The Uganda perspective' Africa Electronic Privacy and Public Voice Symposium (2004).

29 A cultural term commonly used in Southern Africa that defines how an individual exists in a community. U Reviglio & R Alunge '"I am datafied because we are datafied": An ubuntu perspective on (relational) privacy' (2020) 33 *Philosophy and Technology* 595.

30 P Boshe, M Hennemann & R von Meding 'African data protection laws: Current regulatory approaches, policy initiatives and the way forward' (2022) 3 *Global Privacy Law Review*.

31 As above.

32 Universal Declaration of Human Rights art 12.

33 International Covenant on Civil and Political Rights art 17.

34 African Charter on the Rights and Welfare of the Child art 10.

35 AB Makulilo 'The context of data privacy in Africa' in AB Makulilo (ed) *African data privacy laws* (2016) 3.

36 The Constitution of Zimbabwe was published as a Schedule to the Zimbabwe Constitution Order 1979 (SI 1979/1600 of the United Kingdom).

37 G Greenleaf & B Cottier 'Data privacy laws and bills: Growth in Africa, GDPR influence' (2018) *Privacy Laws and Business International Report*; AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) *Computer Law and Security Review* 78.

38 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108).

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

40 Convention 108 (n 38) art 23.

protocol and the Data Protection Directive in Africa are seen continentally and regionally. Continentally, the standards are reflected in the Cyber Security and Personal Data Protection Convention (Malabo Convention) of the African Union (AU).[41] The Malabo Convention establishes regulatory regimes of cybersecurity, electronic transactions and data protection. It harmonises data protection frameworks in AU states, prioritises free movement of data, and ensures the protection of privacy.[42] Zimbabwe is not a signatory to the Malabo Convention. Regionally, the standards are reflected in the Southern Africa Development Community Data Protection (SADC) Model Law.[43] The Model Law is not binding but may be used by SADC states to develop their data protection legislation.

Since the SADC Model Law, there have been developments within the EU with global implications. These are the replacement of Convention 108 with Convention 108+ and GDPR. GDPR is a global benchmark for data protection law[44] and enjoys extraterritorial application.[45] This obliges compliance with the GDPR if African countries engage with digital users in the EU. Countries such as Zimbabwe can comply by either adopting laws and regulations aligned with GDPR or adopting of GDPR-compliant procedures by entities operating in Zimbabwe.[46] The global implications of the GDPR, therefore, cannot be ignored. This influence, however, disregards the unique socio-economic and cultural realities in Africa.[47] The influence of standards developed because of EU legislation in Zimbabwe's data protection Act is presented in Table 1 below. This is done by comparing the standards and provisions of CDPA against the SADC Model law, the Malabo Convention and GDPR. The criteria of the standards used in the comparison stem from the categorisation of them into three levels developed by Greenleaf and Cottier.

41 At the time of writing the Convention is not yet in force. There currently are 13 ratifications, two short of the required 15 for the Convention to enter into force.
42 Convention 108 (n 38) Preamble.
43 Greenleaf & Cottier (n 37).
44 Boshe and others (n 30) 4.
45 Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119, art 3(2)(a).
46 Mannion (n 7) 685.
47 As above.

Table 1 – Comparison of CDPA against data protection standards[48]

First Generation Standards	SADC 2012	AU 2014	GDPR 2016	CDPA
Collection – limited (not excessive), lawful (for legitimate purposes) and by fair means	12	x	5(1)(a)	7(1)(a)
Data quality – relevant, accurate, up to date	11(1)	13(4)	5(1)(d)	7(1)(b)
Purpose specification by time of collection	13	x	5(1)(b)	9(1)
Notice of purpose/rights	21(1)	15	13, 14	15, 16
Uses limited (including disclosures) to purposes specified or compatible	13(1)	13(3)(a)	5(1)(b)	13(c)
Security through reasonable safeguards	24	13(6); 20; 21	5(1)(f), 32	18
Openness re personal data practices (not limited to data subjects)	x	x	14(5)(b)	
Access – individual right of access	31	17	15	14(b)
Correction – individual right of correction	32	19	16, 19	14(d)
Accountable – identified data controller accountable for implementation	x	x	5(1)(f)	24(1)(a)-(b)
Second Generation				
Minimum collection necessary for purpose (data minimisation)	x	10(3)(b)	5(1)(c)	13(d)
Destruction or anonymisation after purpose completed	32(1)(b)	22	5(1)(e)	13(f)
Additional protections for sensitive data in defined categories	15	1 def; 14	9, 10	11, 12
Legitimate bases for processing defined	12, 14	1 def	6	10(2)-(3)
Additional protections on some sensitive processing systems (notification; 'prior checking' by DPA etc.)	26, 28	10(2)-(4)	36	12
Limits on automated decision-making (inclu. right to know processing logic)	31(1c), 36	x	22	25
To object to processing on compelling legitimate grounds	33	18	21	14(c)

48 The table used in this comparison is derived from Greenleaf and Cottier (n 8). It has been modified to include the provisions of the CDPA. The EU Data Protection Directive, C108 and C108+ have been removed from the table.

Restricted data exports requiring recipient country 'adequate', or alternative guarantees	43	14(6)(a)	45-47	28-29
Independent Data Protection Authority(-ies) (DPA)	3(1)	11(1) (b)	51-59, 77	5-6
Recourse to the courts to enforce data privacy rights C108 AP 1(4)	78, 79, 82			x

3rd Generation – Common European Standards	**SADC 2012**	**AU 2014**	**GDPR 2016**	**CDPA**
Data protection by design and by default	x	x	25	x
Demonstrable accountability by controllers	30(1) (b)	x	5(2)	24
Data breach notification to DPA for serious breaches	25	x	33	19
Direct liability for rocessors as well as controllers	x	x	28-31	x
Stronger consent requirements	1(2), 37	x	7, 8	3, 10(1)
Proportionality required in all aspects of processing	x	x	GDPR passim	
DPAs to make decisions and issue administrative santions incl. fines	5(2)	12(2) (h)	58(1)	x
Biometric and genetic data require extra protections	16	104(a), (d)	9	12
Stronger right to erasure incl. 'to be forgotten'	x	19	17, 19	x
DPAs to cooperate in resolving complaints with international elements	x	12(2) (m)	50	x
3rd Generation – GDPR additional standards, 2018 (not in CoE 108+)				
Mandatory Data Protection Impact Assessments (DPIAs) for high-risk processing	x	x	35, 36	x
Extra-territorial jurisdiction, where goods or services offered, or behaviour monitored	x	x	3	4(2)
Extra-territorial controllers or processors must be represented within jurisdiction (EU/other)	x	2(3)	27	4(3)
Right to data protability (UGC/other)	x	23	20	x
Mandatory Data Protection Officers (DPOs) for sensitive processing	x	x	37-39	20(4) (b)-20(6)

Data breach notification to data subjects (if high risk)	x	x	34	x

The Agreement Establishing the African Continental Free Trade Area (AfCFTA) imposes additional data protection obligations on Zimbabwe. According to article 15 of the Protocol on trade in services, member states can enforce and adopt measures 'necessary to secure compliance with law or regulations that are not inconsistent' with the protocol.[49] This includes protection of the privacy of individuals, 'in relation to the processing and dissemination of personal data and the protection of confidentiality of individuals' records and accounts'.[50] The import of article 15 is that members can adopt their own data protection laws if such laws are consistent with the provisions of AfCFTA.[51] The extent of influence of AfCFTA is limited as it remains to be seen how consistency with AfCFTA will be maintained as each member adopts its data protection laws.

4 The Cyber and Data Protection Act of Zimbabwe

4.1 Historical background

CDPA succeeds AIPPA which was Zimbabwe's first data protection legislation. It follows the government's drive to create a technology-driven business environment and encourage technological development while ensuring that technology is used lawfully.[52] The Act targets issues of data protection concerning the Declaration of Rights under the Constitution. It also extends to cyber-related offences, establishing a Cyber Security Centre and a Data Protection Authority and to provide for their functions. The Act further provides for the investigation and collection of evidence of cybercrime and unauthorised data collection and breaches, and for admissibility of electronic evidence for such offences.[53] Before presidential assent, CDPA was criticised for neglecting human rights in regulating personal data protection and being below the minimum standards of modern data protection law.[54] Nonetheless, CDPA constitutes a significant improvement from AIPPA.

AIPPA only applied to public institutions with data processing by private, natural and juristic persons unprotected. Individuals lacked rights associated with

49 Agreement Establishing the African Continental Free Trade Area (AfCFTA) art 15(c).
50 AfCFTA (N 49) art 15(c)(ii).
51 E Salami 'Implementing the AfCFTA Agreement: A case for the harmonisation of data protection law in Africa' (2022) 1 *Journal of African Law* 285.
52 CDPA (n 1).
53 As above.
54 Media Institute of Southern Africa 'Cybersecurity and Data Protection Bill entrenches surveillance' 19 May 2020, https://zimbabwe.misa.org/2020/05/19/cybersecurity-and-data-protection-bill-entrenches-surveillance-an-analysis/ (accessed 6 December 2021).

data protection legislation against private persons. AIPPA also only provided for a right to correction.[55] AIPPA was unsuitable as a regulatory framework for data protection.[56] CDPA, thus, is an attempt to fix the shortcomings of AIPPA while ensuring that Zimbabwe satisfies the minimum threshold of data protection and also ensure the transfer of data from other nations to the country. Nonetheless, CDPA contains pitfalls that may undermine the protection of personal data.

4.2 Definitions

This part considers the key terms in the Act whose interpretation is crucial to the protection of the rights of data subjects.

4.2.1 Personal information

Personal information is at the core of CDPA. However, the term as defined fails the comprehensibility test, which entails not only the language used to make an act understandable but its readability. It is broken down into three definitions, namely, 'personal information', 'data subject' and 'identifiable person'. 'Personal information' is defined as 'information relating to a data subject'.[57] A 'data subject' is defined as 'an individual who is an identifiable person and the subject of data'. An 'identifiable person' is defined as a person who can be identified directly or indirectly in particular reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.[58] Personal information, therefore, is any information relating to an identified or identifiable person who can be identified, directly or indirectly, by reference to an identifier, which includes an identification number.

CDPA applies only to natural persons. Only natural persons are addressed using gender pronouns and have specific physical, physiological, mental and cultural identities. A key phrase from the definition formulated by this article is 'information relating to an identified or identifiable natural person'. A person is identifiable if one considers all the means reasonably likely to be used by a controller or other person to identify the natural person directly or indirectly.[59] Information, therefore, will not relate to an individual where a disproportionate effort is required to identify the individual. The concept of personal data, however, now is more dynamic. Without additional effort, anonymised data

55 AIPPA (n 4) part IV & part V.
56 Ncube (n 15) 99.
57 This includes a person's name, address or telephone number.
58 CDPA (n 1) sec 2.
59 M Finck & F Pallas 'They who must not be identified – Distinguishing personal from non-personal data under the GDPR' (2020) 10 *International Data Privacy Law* 11-36; Recital 65 GDPR.

remains non-personal data, but the economic and technological trends portend for less of a distinction.[60]

4.2.2 Data

The CDPA defines data as

> any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data.[61]

This creates ambiguity about the scope of CDPA. Section 4 resolves this quandary by providing that CDPA applies to matters relating to the processing and storage of data. 'Processing' is defined as 'any operation or set of operations which are performed upon data, whether or not by automatic means, such as obtaining recording or holding the data or carrying out any operation or set of operations on data'. This creates a strong supposition that non-personal information is within the scope of CDPA, which is atypical of data protection legislation. This ambiguity could have been resolved by the insertion of 'data subject' or by altogether removing the definition of data.

If the above supposition is correct, controllers, processors and the data protection authority (DPA) will have additional responsibilities because of non-personal information. This, however, creates compliance fatigue. Entities will seek a compliance balance between personal and non-personal information. This is worsened by the inclusion of 'information' in the definition of 'data' as the distinction between information and data might be too technical. The result undermines the objectives of CDPA. The inclusion of non-personal information as a subject of regulation, however, might have been an attempt by the legislature to harmonise personal and non-personal information.[62] This is important as technology has blurred the boundary between personal and non-personal.[63]

4.3 Application of the Act

CDPA applies to access to information, protection of privacy of information, and the processing and storage of data.[64] The territorial scope of CDPA stands

60 As above.
61 CDPA (n 1) sec 3.
62 J Drexl 'Legal challenges of the changing role of personal and non-personal data in the data economy' in A di Franceschi & R Schulze (eds) *Digital revolution – New challenges for law: Data protection, artificial intelligence, smart products, blockchain technology and virtual currencies* (2019) 19-41.
63 As above.
64 CDPA (n 1) sec 4.

on an 'establishment' and a 'means' criterion.[65] While the Act does not use 'establishment' in section 4(2)(a), it is apparent that the legislature intended an 'establishment' criterion. According to section 4(2)(a), CDPA applies to the processing of data in the 'effective and actual activities of any data controller'. This seems to derive from Recital 22 of GDPR, which provides that '[e]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.'

Recital 22 aids the interpretation of the GDPR establishment criterion. As such, the first territorial criterion is one of 'establishment'. The use of the words 'effective and actual' suggests a departure from the traditional notion of establishment focusing on the entity's place of registration.[66] CDPA applies where a data controller has some stability within Zimbabwe and where the nature of the services offered and the economic activity undertaken are within Zimbabwe. An example is services exclusively offered over the internet.

Evidence of the means criterion is in section 4(2)(b), which provides that it applies to the processing of data by a controller who is not established in Zimbabwe where the means used is in Zimbabwe.[67] The requirement of whether processing occurred by means in Zimbabwe must be assessed when the relevant trigger activity occurs. This would ordinarily be the moment the good or service is offered to the data subject. The provision is aimed at activities deliberately using means in Zimbabwe to process data. As such, where processing and storage of data are undertaken by a controller with Zimbabwe being a data transit, CDPA is inapplicable.[68]

The Act is silent as to where it is inapplicable, yet it has become customary for data protection legislation to define its scope and exceptions. Data protection legislation can be an anathema to the enjoyment of people's rights, particularly in the digital age where individuals conduct some form of processing of personal data.[69] This is why the SADC Model Law, the Malabo Convention and GDPR exclude processing for purely personal or domestic purposes. The Malabo Convention further excludes processing for artistic and literary expressions and journalistic purposes within professional codes of conduct. Not every act of data processing by an individual invokes the application of data protection law. Such an approach would make data protection law oppressive and tedious to apply.[70]

65 European Data Protection Board 'Guidelines 3/2018 on the Territorial Scope of the GDPR' (Article 3) – Version Adopted after Public Consultation; O Saki 'Guide to the Zimbabwean Cyber And Data Protection Act', https://data.misa.org/en/entity/28jfydpjr4c (accessed 16 June 2022).
66 *Weltimmo v Hungarian National Authority for Data Protection and Freedom of Information* (C230/14).
67 CDPA (n 1) sec 4(2)(b).
68 As above.
69 A Murray *Information technology law* (2018).
70 As above, 583.

With more people spending time online, CDPA should exclude processing outside professional or commercial activity.[71] It must include a provision exempting processing for domestic or household activities. The scope and interpretation of the exception would then be left to the courts through interpretative guidance given by the DPA in line with the decisions in *Lindqvist*[72] *and Rynes.*[73]

4.4 Data protection authority

CDPA designates the Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ) as the data protection authority (DPA)[74] responsible for the enforcement of CDPA. POTRAZ is established under section 3 of the Postal and Telecommunications Act.[75] Its major function is to 'ensure the provision of sufficient domestic and international telecommunication and postal services throughout Zimbabwe on such terms and conditions as the Authority may fix'.[76] POTRAZ is run by a board appointed by the President after consultation with the responsible minister.[77] The functions of POTRAZ as a DPA are contained in section 6 of CDPA. These include regulating the processing of personal information, by establishing conditions for lawful processing;[78] the promotion and enforcement of fair processing;[79] and the issuing of opinions on matters relating to the application of the Act on its own accord or at the request of a person with a legitimate interest.[80]

POTRAZ may submit to any court any administrative action that is not compliant with the fundamental principles of CDPA and any law on the protection of privacy concerning the processing of data.[81] POTRAZ, however, must first consult the Minister responsible for Information, Publicity and Broadcasting Services.[82] POTRAZ is responsible for conducting inquiries or investigations either of its own accord or at the request of a data subject or interested person.[83] It must also ensure that feedback is given to the complainant.[84] It is responsible for researching policy and legal matters about international best practices on the protection of personal information and facilitating cross-border cooperation in the enforcement of privacy laws.[85] POTRAZ is mandated to provide guidelines and approve codes of conduct and ethics governing rules of conduct for data

71 GDPR (n45) Recital 18.
72 Case C-101/01 *Bodil Lindqvist* [2003] ECLI:EU:C:2003:596.
73 Case C-212/13 *Rynes v Urad pro ochranu osobnich udaju* [2014] ECLI: EU:C:2014:2428.
74 CDPA (n 1) sec 5.
75 Postal and Telecommunications Act (PTA) [Chapter 12:05] Act 4 of 2000.
76 PTA (n 75) sec 4.
77 PTA (n 75) sec 5.
78 CDPA (n 1) sec 6(1)(a).
79 CDPA (n 1) sec 6(1)(b).
80 CDPA (n 1) sec 6(1)(c).
81 CDPA (n 1) sec 6(1)(d).
82 As above.
83 CDPA (n 1) sec 6(1)(f).
84 CDPA (n 1) secs 6(1)(a)-(h).
85 CDPA (n 1) secs 6(1)(i)-(j).

controllers. Controllers desiring to have codes of conduct approved must submit them to POTRAZ for ascertaining compliance with CDPA. In deciding whether to approve a code of conduct, the DPA can consult data subjects or their representatives.[86]

POTRAZ was established as an independent body.[87] The independence, however, is worth evaluating as it is essential for protecting personal information. This is important in the Zimbabwean context where there have been incidents of abuse of personal information by political parties during campaigns, and by the government.[88] In evaluating the independence of POTRAZ, reliance will be placed on attributes of independent data protection supervisory authorities identified by Greenleaf in his study of international instruments on the independence of data protection authorities.[89] These include (i) the establishment of the authority by legislation rather than executive order or delegated legislation; (ii) the ability to investigate and report free of direction or permission from any other political or governmental authority; (iii) a fixed term of office to avoid a commissioner being at the whim of the executive; (iv) removal from office only for defined reasons and with procedural safeguards; and (v) powers and duties to report directly on issues, either to Parliament or to inform the public of its activities.

Other key factors influencing independence include immunity from personal lawsuits against commissioners for conduct relating to the performance of duties; independent determination of resources; positive qualification requirements for commissioners; the prohibition on commissioners to undertake other concurrent positions the prohibition on the appointment of commissioners from specified backgrounds with potential conflicts of interests; decisions of the authority being subject to a right of judicial appeal and review; and the personal character of the commissioner. The factors influencing independence are similar to the factors safeguarding independent commissions created under chapter 12 of the Zimbabwean Constitution. The similarity of the attributes by Greenleaf and the safeguards makes them ideal for evaluating the independence of POTRAZ.

The independence of POTRAZ is compromised. First, POTRAZ remains under government control. In terms of its establishing Act, the minister may direct the POTRAZ board on policies that the minister deems necessary for the national interest.[90] The minister may also direct the board to reverse, suspend or rescind its decisions or actions. The only requirement for interference is that the minister must satisfy themselves that there are reasonable grounds that the decision or action is not in the national or public interest.[91] What constitutes

86 CDPA (n 1) sec 30(4).
87 CDPA (n 1) sec 6(2).
88 Maunganidze (n 6).
89 G Greenleaf 'Independence of data privacy authorities: International standards and Asia Pacific experience' (2012) 28 *Computer Law and Security Review* 3.
90 PTA (n 75) sec 25.
91 PTA (n 75) sec 26.

national or public interest is not defined in the Postal and Telecommunications Act (PTA), thus creating broad powers for interference. An example of this is provided by section 11(4) of CDPA which provides that the Minister of State Security, in consultation with the minister responsible for information and communications technologies,can give directions on the implementation of the Act in respect of sensitive information affecting national security or the interests of the state. This undermines the independence of POTRAZ as a DPA.

CDPA does not exclude decisions made by the POTRAZ board on the functions of a DPA from interference by the minister. It does not describe how POTRAZ will function as a DPA and whether it will be a division within POTRAZ. Being a separate division means that the decisions and actions of the DPA will be subject to reversal, suspension or rescission by the minister. Any investigation that it may want to undertake against the government would be interfered with. POTRAZ, therefore, will be unable to investigate matters without direction or permission from the minister. While section 6(2) of CDPA excludes anyone from giving directives to POTRAZ as a DPA, this is not convincing. There are provisions in CDPA, such as section 11(4) demonstrating that POTRAZ will operate under directives on national security interests, and these issues ignite possibilities of state-sanctioned surveillance. This is concerning, with data transfers for jurisdictions such as the EU considering decisions such as *Schrems* I[92] and II.[93]

The board's independence is also compromised by the terms and conditions of service, which are determined by the President.[94] Board members, thus, are prone to manipulation by the appointing authority. Where board members act contrary to the expectations of the appointing authority, they may be dismissed or subsequent appointments may be threatened with unfavourable terms and conditions of service, undermining their independence. Moreover, there is poor security against removal as they may be removed from their positions on mere allegations. Board members are simply required to make representations but may be dismissed despite the representations.[95] This further undermines their security of tenure. An example is the 2014 POTRAZ board that was dismissed on allegations of corruption and poor corporate governance.[96] However, there are counter-allegations that, instead, the board was dismissed because the then Minister of Information Communication Technology wanted to appoint a

92 Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650.
93 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559.
94 PTA (n 75) sec 7.
95 PTA (n 75) sec 10.
96 F Munyoro 'Potraz board fired over graft ' *The Herald* 3 July 2015, https://www.herald.co.zw/potraz-board-fired-over-graft/ (accessed 27 March 2023).

board amenable to his instructions.[97] This lack of security of tenure, therefore, significantly impacts the independence of POTRAZ in its supervisory functions.

CDPA is similarly silent on how POTRAZ in its supervisory function will be funded. The funding will be from the executive as POTRAZ is under governmental control. Funds will thus be given to POTRAZ as an entity and then distributed to its several functions, including the data protection supervisory function. This may cause problems given that POTRAZ will have to balance its two roles, being a telecommunications regulator and a DPA. Government funding will be inadequate for POTRAZ to diligently fulfil these functions. Financial independence is essential for a DPA to effectively conduct investigations and carry out its responsibilities.[98] Without financial independence, the effectiveness of POTRAZ is questionable. Further, CDPA is silent on the recruitment of staff working in the DPA function. The failure to stipulate criteria and conditions for staff employment potentially creates questions on their partiality based on who eventually appoints them, how they will be appointed, and under what conditions. Arguably, the designation of POTRAZ as a data protection authority is also against the rules of natural justice as POTRAZ essentially is a judge, jury and executor in its own cases where it acts as a data controller in carrying out its regulatory function.

While the above concerns remain possibilities, the legislature could have done more to ensure the independence of the supervisory function. There was a need to have a stand-alone institution akin to constitutional commissions that would be established by CDPA and given a status similar to constitutional commissions.[99] Constitutional commissions' objectives include supporting and entrenching human rights and democracy; protecting the sovereignty and interests of the people; promoting constitutionalism; promoting transparency and accountability; and ensuring that injustices are remedied.[100] The general objectives of independent commissions are like those of a DPA.[101] Thus, with the same status as a constitutional commission, the DPA would be empowered to employ staff and regulate their terms of service.[102] It would have its independence guaranteed,[103] with members of staff being non-political. The staff members would then be appointed by the President after they have been interviewed by Parliament. They would then enjoy security of tenure.[104] Another proposal

97 This allegation is made by Reward Kangai, former CEO of NETONE in a series of tweets that can be seen at https://twitter.com/rewardkangai/status/1344989184885469184?s=21 (accessed 26 March 2023).
98 Greenleaf (n 89).
99 These include the Zimbabwe Human Rights Commission; Zimbabwe Electoral Commission; Zimbabwe Media Commission; Zimbabwe Gender Commission; and National Peace and Reconciliation Commission.
100 Constitution of Zimbabwe (n 12) sec 233.
101 *Commission v Germany* (2010) (OJ C 113 of 01.05.2010. The case stipulated the general objective of a supervisory authority and its importance.
102 Constitution of Zimbabwe (n 12) sec 234.
103 Constitution of Zimbabwe (n 12) sec 235.
104 Constitution of Zimbabwe (n 12) sec 237(3).

is to mandate the Zimbabwe Media Commission (ZMC), responsible for administering the Freedom of Information Act.[105] This mirrors the South African approach where the Protection of Personal Information Act (POPIA)[106] and the Promotion of Access to Information Act (PAIA)[107] are under the Information Regulator.

4.5 Obligations of data controllers and processors

A data controller is a natural or legal person licensable by POTRAZ, who determines the purpose and means of processing.[108] A data processor processes data for the data controller under the instruction of the controller.[109] Persons under the direct employment or authority of a data controller are not considered processors. Processing is any operation performed upon data, whether or not by automatic means. It includes obtaining, recording, holding, organising, adaptation, alteration, retrieval, consultation, alignment, combining, blocking or erasure of data. CDPA has three tiers of obligations applicable to data controllers and processors. The first tier consists of specific rules on data quality applicable to data controllers.[110] The second tier consists of general rules applicable to both data controllers and processors when processing data.[111] The third tier consists of rules relating to the processing of personal information, applicable to data controllers and processors.[112] Each of the tiers is discussed below.

First-tier obligations relate to data quality with data controllers being required to ensure that processing is adequate, relevant and not excessive regarding the purpose for which it is collected.[113] Data processed must be accurate, current, and retained in a form allowing identification of data subjects for periods no longer than is necessary for the purpose for which it was collected.[114] It must be accessible regardless of the technology used, and technological evolution must not hinder the accessing or processing of such data.[115] CPDA, however, does not stipulate who is entitled to access the data. The presumption is that it should be accessible to the data subject as it is collected from them.

Second-tier obligations relate to lawfulness and fairness. Data must be processed only where necessary, fairly and lawfully.[116] It must be for a specific, explicit and legitimate purpose and must not be further processed in a way that

105 (FoIA) [Chapter 10:23] 1 of 2020.
106 Protection of Personal Information Act 4 of 2013.
107 Promotion of Access to Information Act 2 of 2000.
108 CDPA (n 1) sec 2.
109 As above.
110 CDPA (n 1) sec 7.
111 CDPA (n 1) secs 8-12.
112 CDPA (n 1) sec 13.
113 CDPA (n 1) sec 7(1)(a).
114 CDPA (n 1) secs 7(1)(b)-(c).
115 CDPA (n 1) sec 7(2).
116 CDPA (n 1) sec 8.

is incompatible with the purpose of its collection.[117] POTRAZ can specify conditions where further processing of data for historical or scientific research purposes is compatible with the original processing purpose.[118] These obligations are reinforced as duties of a data controller in section 13 of CDPA. The second tier also imposes rules on the processing of non-sensitive personal information,[119] sensitive personal information,[120] genetic data, biometric sensitive data and health data.[121] These rules provide a legal basis for the processing of data.

Third-tier obligations are in the form of duties imposed on the data controller or processor. These duties mirror the principles of the processing of personal data in international data protection instruments and leading data protection instruments.[122] As such, interpretation or guidance on these principles may be used in interpreting the general duties imposed by CDPA. The first duty requires personal information to be processed in accordance with the right to privacy of the data subject.[123] This means that the protection of personal information is premised on the right to privacy. The second duty requires personal information to be processed lawfully, fairly and transparently.[124] Data subjects, therefore, must be informed beforehand about what will be done with their personal information. The duty placed on administrative authorities processing personal information mirrors the 'to act lawfully'.[125] To lawfully process personal information, data controllers and processors can rely on the different lawful processing conditions provided in CDPA.[126]

The third duty requires the collection of personal information to be for an explicit, specific and legitimate purpose, and processing must be compatible with the purpose.[127] Thus, when personal information is collected for a specific purpose, for example, billing, it must not be used for other purposes such as marketing unless the data subject has approved it or if a lawful basis exists. The fourth duty requires the collection of personal information to be limited to what is necessary for the purpose for which it is processed.[128] The fifth duty requires that a valid explanation be provided before the collection of personal information relating to family or private affairs.[129]

117 CDPA (n 1) sec 9(1).
118 CDPA (n 1) sec 9(2).
119 CDPA (n 1) sec 10.
120 CDPA (n 1) sec 11.
121 CDPA (n 1) sec 12.
122 An example is GDPR (n 45) art 5.
123 CDPA (n 1 above) sec 13(a).
124 CDPA (n 1) sec 13(b).
125 Constitution of Zimbabwe (n 12) sec 68(1); Administrative Justice Act [Chapter 10:28] 12 of 2004 sec 3.
126 These include consent, legitimate interest, performance of a contract.
127 CDPA (n 1) sec 13(c).
128 CDPA (n 1) sec 13(d).
129 CDPA (n 1) sec 13(e).

The sixth duty requires personal information to be accurate and, where necessary, current. Reasonable steps must be taken to ensure that any inaccurate personal data is promptly erased or rectified.[130] This requires data controllers and processors to have mechanisms that ensure quick investigation, identification and action on any reported inaccuracies. Data controllers and processors must ensure that personal information is kept in a form identifying the data subject 'for no longer than is necessary for the purposes which it was collected'.[131] Thus, the duration for which personal information is kept by organisations should be given due regard and, where it is no longer necessary, organisations must ensure that they delete personal information.

4.6 Transparency of processing

To ensure transparency of processing, CDPA imposes disclosure obligations on controllers. When data is obtained directly from the data subject, they must be provided with information such as the name and address of the controller and the representative if any;[132] the purpose of the processing;[133] the existence of a right to object to the processing of data if it is obtained for direct marketing;[134] whether compliance with the request for information is compulsory; and consequences of non-compliance.[135] Supporting information may be provided in appropriate circumstances and includes recipients or categories of recipients of data, whether it is compulsory to reply, and the existence of the right to access and rectify data.[136] Similar obligations apply when data has not been collected directly from the data subject.[137] However, there are additional disclosure requirements when data is obtained from third parties for direct marketing. The data controller must first ensure that the data subject is notified of the right to object to the processing of data.[138]

POTRAZ may specify additional information to be provided when data is collected directly from a data subject.[139] No guidance or additional specification has to date been provided by POTRAZ. CDPA lacks comprehensive transparency requirements for data subjects, as there is no obligation to inform them of their right to complain to the DPA or of the period in which their personal information will be stored. Data controllers must also inform data subjects as to how they can exercise their rights, and the limitations on the rights. CDPA imposes transparency obligations on data controllers but they have a discretion

130 CDPA (n 1) sec 13(f).
131 As above.
132 CPDA (n 1) sec 15(1)(a).
133 CDPA (n 1) sec 15(1)(b).
134 CDPA (n 1) sec 15(1)(c).
135 CDPA (n 1) sec 15(1)(d).
136 CDPA (n 1) sec 15(1)(e).
137 CDPA (n 1) sec 16(1).
138 CDPA (n 1) sec 16(1)(d).
139 CDPA (n 1) sec 16(1)(f).

on compliance with disclosure obligations, with the most common method being privacy notices.[140] Most of the privacy notices, however, are complex to read.[141] Arguably, they simply ensure compliance with legal requirements as opposed to showing data subjects how their data is used.[142] Thus, more could have been done to ensure that disclosure is made more simply. Given that POTRAZ has the authority to issue guidance and regulate how disclosures can be made, there is room to ensure that privacy notices adopted using plain and simple language. POTRAZ can also require the use of machine-readable language by controllers as a way of ensuring greater transparency. Disclosure obligations, however, are not absolute. Data controllers are exempted from notifying the data subject when data has not been acquired from the subject if informing them would involve a disproportionate effort or is impossible.[143] Further exemptions apply when data is collected for statistical and research purposes or when it has been collected for medical examination to protect and promote public health.[144] Disclosure is also exempted when data is obtained from a third party or when it has been provided in terms of a law.[145]

Apart from disclosure obligations to data subjects, data controllers have disclosure obligations to POTRAZ. They must notify POTRAZ before carrying out any wholly or partly-automated operation or set of operations that intend to serve a single purpose or several related purposes.[146] However, an exception applies where the operations have the sole purpose of keeping a register intended to provide information to the public by law and that is accessible by the public.[147] POTRAZ may further exempt certain categories from notification where it has considered the data being processed and that there is no risk of infringement of data subjects' rights and freedoms.[148] POTRAZ must also be informed of the purposes of the processing, categories of data being processed, categories of data subjects, categories of recipients, and the retention period[149] for the exemption to apply. Furthermore, the data controller must appoint a data protection officer (DPO)[150] and POTRAZ must be notified of his appointment. POTRAZ

140 J Mohan, M Wasserman & V Chidambaram 'Analysing GDPR compliance through the lens of privacy policy' in V Gadepally and others (eds) *Heterogeneous data management, polystores, and analytics for healthcare* (2019) 82.

141 A Terpstra and others 'Improving privacy choice through design: How designing for reflection could

support privacy self-management' *First Monday* (2019), https://journals.uic.edu/ojs/index.php/fm/article/view/9358 (accessed 7 December 2021); S Jordan, S Narasimhan & J Hong 'Deficiencies in the disclosures of privacy policies and in user choice' *Social Science Research Network* (2021), https://papers.ssrn.com/abstract=3894548 (accessed 7 December 2021).

142 Mohan and others (n 140).

143 CPDA (n 1) sec 16(2)(a).

144 As above.

145 CPDA (n 1) sec 16(2)(b).

146 CPDA (n 1) sec 20(1).

147 CPDA (n 1) sec 20(2).

148 CPDA (n 1) sec 20(4)(a).

149 As above.

150 CPDA (n 1) sec 20(4)(b).

stipulates the minimum qualifications and functions of the DPO.[151] The CDA requires data controllers to ensure that the DPO is free to conduct its duties including ensuring compliance, dealing with requests made to the data controller, and working with POTRAZ.[152]

Where a data controller is not exempted from notifying POTRAZ, the notification must contain the date of notification and the law permitting the automatic processing,[153] full names, complete address, and registered office of the data controller and the representative where there is one.[154] The data controller must also inform the purpose of automatic processing, categories of data being processed including a detailed description of the sensitive data being processed; category or categories of data subjects; safeguards to be linked to disclosure of data to third parties; manner in which data subjects are informed and service providing a right to access and a measure taken to facilitate the right. POTRAZ must be notified of the period after the expiration of which data may no longer be stored; recourse to the data processor, if any; transfer to a third country and an assessment of whether security measures provided are adequate.[155] POTRAZ may prescribe other information that must be provided by the data controller.

4.7 Security of processing

CDPA requires that data controllers and processors or their representatives adopt appropriate technical and organisational measures protecting the data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or processing, or access.[156] The rationale for this is to safeguard the integrity, security and confidentiality of the data. The measures must ensure an appropriate level of security.[157] POTRAZ may issue standards it considers appropriate concerning information security for all or certain categories of processing.[158] POTRAZ is also empowered to inspect and assess the security and organisational measures before the commencement of processing or transfer of data where it formulates an opinion that processing or transfer of data by a data controller entails specific risk to the privacy or rights of data subjects.[159] Where a data controller seeks to appoint a data processor, they must ensure that the data processor can provide

151 POTRAZ in The Postal and Telecommunications Regulatory Authority of Zimbabwe [Public Notice on Data Protection Act Chapter 11:20] 5 of 2021. Public Notice Number 1 of 2022 provides for the qualification of a person with no less than an advanced level certificate of education.
152 CDPA (n 1) sec 20(6).
153 CPDA (n 1) sec 21(1)(a).
154 CPDA (n 1) sec 21(1)(b).
155 CPDA (n 1) sec 21(1).
156 CPDA (n 1) sec 18(1).
157 CPDA (n 1) sec 18(2).
158 CPDA (n 1) sec 18(3).
159 CPDA (n 1) sec 21(3).

sufficient guarantees regarding technical and organisational security measures to protect data.[160]

The data processor, therefore, may only process data following the instructions from the data controller.[161] The data processor and the data controller must enter into a written contract ensuring that the data processor maintains security measures on the data being processed.[162] Where there has been a security breach, the data controller is obliged to notify POTRAZ within 24 hours.[163] The notification period given to data controllers when a breach has occurred is insufficient. It could take controllers more than 24 hours to identify the exact scope of the breach. As a result, every security incident a data controller detects will be reported, potentially overwhelming POTRAZ. There is also a risk that security incidents will be downplayed and there will be underreporting to POTRAZ. Ideally, CDPA should have adopted the international standard period of 72 hours. While there is a requirement to notify POTRAZ of a data breach, there is no separate requirement to notify the data subject in circumstances of potentially high risk to the rights and freedoms of the data subject.

4.8 Accountability

Under CDPA data controllers must take all measures necessary to demonstrate compliance with the principles and obligations set out.[164] This often is referred to as the accountability principle. Data controllers must have internal mechanisms in place for demonstrating compliance to both data subjects and POTRAZ in the exercise of their powers. The accountability principle demands that there is a demonstration of compliance with all provisions of CDPA, and not only sections that might be framed as specific to data controllers.

4.9 Legal basis for the processing of data

CDPA provides several lawful bases for processing non-sensitive personal information. The first is with the consent of the data subject or a competent person where the data subject is a child.[165] Consent is the specific, unequivocal, freely given, informed expression of will by a data subject or their legal, judicial or legally-appointed representative to have their data processed.[166] Consent may be implied if the data subject is an adult or has a legal persona and full legal capacity to consent.[167] However, there is no mention of the circumstances where consent

160 CPDA (n 1) sec 18(4).
161 CPDA (n 1) sec 17.
162 CPDA (n 1) sec 18(5).
163 CPDA (n 1) sec 19.
164 CPDA (n 1) sec 18(3).
165 CPDA (n 1) sec 10(1).
166 CPDA (n 1) sec 3.
167 CPDA (n 1) sec 10(2).

may be implied from the data subject. This defeats the whole notion of consent as it is a mechanism of people exercising control over whom they decide to share their information with. This is more so when CDPA provides that personal information may only be processed where the data subject consents.[168]

Processing without consent is permissible where the data is key in proving an offence;[169] where the data controller must comply with an obligation to which the controller is subject or by law;[170] protecting the vital interests of the data subject;[171] or where the data controller is performing a task in the public interest or in the exercise of official authority vested in the controller or a third party to whom the data is disclosed.[172] Consent also is unnecessary where processing is meant to promote the legitimate interests of the controller or a third party to whom data is disclosed.[173] However, legitimate interest cannot be relied on where the legitimate interests of the controller are overridden by the interests or fundamental rights and freedoms of the data subject.[174] POTRAZ may specify conditions when legitimate interest is considered to have been met.[175]

Processing of sensitive data without the data subject's consent is prohibited.[176] Sensitive data is information or any opinion revealing the racial or ethnic origin, political opinions and affiliations, religious and philosophical beliefs of a data subject. It also includes membership of a professional or trade association; membership of a trade union; sex life; criminal, educational, financial or employment history; gender, age, marital status, family status; health information, genetic information; and any information presenting major risks to a data subject. Where a data subject consents to the processing of sensitive data, such consent may be withdrawn without explanation.[177] POTRAZ, however, can prohibit the processing of sensitive data even where the data subject consents.[178]

Where the processing of sensitive data may affect national security or the interests of the state, the minister responsible for cybersecurity may direct how sensitive information must be processed.[179] Written consent is unnecessary to process sensitive data where processing is required to carry out obligations and specific rights of a data controller in the field of employment law,[180] and where it is necessary to protect vital interests of the data subject where they are unable to

168 CPDA (n 1) sec 10(1).
169 CPDA (n 1) sec 10(3)(a).
170 CPDA (n 1) sec 10(3)(b).
171 CPDA (n 1) sec 10(3)(c).
172 CPDA (n 1) sec 10(3)(d).
173 CPDA (n 1) sec 10(3)(e).
174 As above.
175 CPDA (n 1) sec 10(4).
176 CPDA (n 1) sec 11(1).
177 CPDA (n 1) sec 11(2).
178 CPDA (n 1) sec 11(3).
179 CPDA (n 1) sec 11(4).
180 CPDA (n 1) sec 11(5)(a).

consent.[181] Written consent is unnecessary where processing is carried out during legitimate activities of a foundation, association or non-profit organisation.[182] The foundation or non-profit organisation must have a political, philosophical, religious, health insurance or trade union purpose. The processing must also relate solely to the members of the organisation or people who have regular contact with the organisation. The data controller must obtain the consent of the data subject before sharing sensitive data.

Sensitive data can be processed without consent if the processing is for compliance with national security laws;[183] is necessary for the establishment, exercise or defence of legal claims;[184] if it relates to data that has been made public by the data subject;[185] where processing is necessary for scientific research;[186] or if the processing is authorised by law or any regulation.[187] Data relating to sex life may be processed without consent by an association with a legal personality or by a public interest organisation whose main objective is the evaluation, guidance or treatment of a person of certain sexual conduct.[188] The organisation must be recognised by a competent public body as being responsible for the welfare of such persons. The objective of the processing by the organisation must consist of evaluation, guidance and treatment of persons.[189]

Genetic, biometric and health data must also be processed with the written consent of the data subject. The exceptions to this also apply to the processing of genetic data, biometric data and health data.[190] Health data, however, may only be processed under the responsibility of a healthcare professional.[191] Healthcare professionals and their agents are bound by the duty of professional secrecy.[192] An exception is if the data subject consents in writing, and it is necessary for the prevention of imminent danger or mitigation of a specific offence.

CDPA prohibits the collection of health data from other sources unless the data subject is incapable of providing the data.[193] Health-related data, however, must only be processed where a unique patient identifier is given to the patient. This patient identifier must be distinct from any other identification number issued by the public authority, for example, a national identity number or a passport number. The linking of the unique patient identifier with other identifiers that

181 CPDA (n 1) sec 11(5)(b).
182 CPDA (n 1) sec 11(5)(c).
183 CPDA (n 1) sec 11(5)(d).
184 CPDA (n 1) sec 11(5)(e).
185 CPDA (n 1) sec 11(5)(f).
186 CPDA (n 1) sec 11(5)(g).
187 CPDA (n 1) sec 11(5)(h).
188 CPDA (n 1) sec 11(5)(i).
189 CPDA (n 1) sec 11(5)(j).
190 CPDA (n 1) secs 12(3)(a)-(j).
191 CPDA (n 1) sec 12(4).
192 CPDA (n 1) sec 12(7).
193 CPDA (n 1) sec 12(6).

may result in the identification of the data subject is prohibited. An exception to this prohibition is when there has been express authorisation by POTRAZ.[194]

4.10 Incomplete obligations

CDPA is not explicit on some of the critical obligations on data controllers, which have become standard in data protection legislation around the world. GDPR, in particular, clearly articulates these principles.[195] This is a missed opportunity to strengthen the protection of personal information by CDPA. The first of such obligations is data protection by design. Data protection by design ensures that data protection principles are implemented, and the necessary safeguards are in place when an information technology system is designed.[196] At the core of data protection by design is the idea that data protection must be inscribed into the design of information technologies from the outset. The second modern principle is that data protection must be by default. This principle is assumed in the various CDPA provisions but is not explicitly stated.[197]

This ensures that only necessary data is collected and processed by data controllers. Data protection by design and default constitutes a shift to a proactive model of data protection aimed at preventing data protection issues instead of remedying them. The failure of CDPA to include an obligation of ensuring data protection by design and default means that CDPA adopts a reactive model to data protection as its provisions are meant to deal with issues of data breaches and other data protection-related matters when they occur. Closely related to the issue of data protection by design and default is the concept of privacy and data protection impact assessments. These are processes 'designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them'.[198] There is no requirement for controllers to carry out privacy and data protection impact assessments before releasing a product significantly involving the collection and processing of personal data.

Impact assessments enable controllers to rethink data processing. They provide controllers with an opportunity to comply with data protection legislation and

194 CPDA (n 1) sec 12(8).
195 GDPR arts 25(1) & (2)
196 European Data Protection Board 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default Version 2.0 Adopted on 20 October 2020'.
197 The CDPA provides in secs 18(1)-(4) on security measures that data controllers can adopt. These measures take into account the state of technological development and the cost of implementing the measures, on the one hand, and the nature of the data to be protected. This provision is helpful but not sufficient, as a data controller has room to manoeuvre, especially using costs as a factor.
198 Article 29 Working Party 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679' 4.

demonstrate appropriate measures taken to ensure legal compliance.[199] It is yet to be seen if POTRAZ with its broad powers to issue guidelines will make impact assessments mandatory. If POTRAZ seeks to make impact assessments mandatory, it should ideally compile lists inclusive of when it considers it necessary for a data controller to carry out an impact assessment and those circumstances that do not require impact assessments. An impact assessment would also enable controllers realising high risk to ensure that there is prior consultation with POTRAZ and data subjects to ensure that the processing does not result in an infringement of fundamental rights.

4.11 Rights of data subjects

CDPA provides for the rights of data subjects. The first is the right to be informed of how their personal information is used.[200] This must be done at the time of collection of data by the data controller.[201] The second is a right of access to personal information held by a data controller or data processor.[202] This right is exercised under the Freedom of Information Act (FOIA) as well, which is administered by a constitutional commission, and the timelines listed there might apply, but there might be conflicts between ZMC and POTRAZ on a request. However, there is no provision on the timeframe within which the data controller or data processor must comply with the request for access in CDPA and, therefore, provisions of FOIA apply. Furthermore, CDPA does not describe the nature and scope of the right. This means that it will be up to the POTRAZ to issue guidance on the nature of the right of access and what it entails. Other rights include a right to object to the processing of all or part of personal information;[203] a right to correction of false or misleading personal information;[204] and a right to deletion of false or misleading data about them.[205]

Data subjects have a right not to be subjected to a decision based solely on automated processing and profiling where the processing or profiling produces legal effects on the data subject and affect them.[206] Automated processing is permissible where the data subject consents or where the processing is premised on a provision established by law.[207] However, some data subject rights which have become standard in international data protection law are not provided for by CDPA. The first of such rights is the right to erasure, commonly known as the right to be forgotten. While there is a right to deletion in CDPA, it is limited to the deletion of false or misleading data and excludes correct personal information.

199 As above.
200 CPDA (n 1) sec 14(a).
201 CPDA (n 1) sec 15(1)(b).
202 CPDA (n 1) sec 14(b).
203 CPDA (n 1) sec 14(c).
204 CPDA (n 1) sec 14(d).
205 CPDA (n 1) sec 14(e).
206 CPDA (n 1) sec 25(1).
207 CPDA (n 1) sec 25(2).

The right to erasure constitutes a fundamental safeguard for the enforcement of data protection principles, especially the principle of data minimisation. The right to erasure is not absolute and usually has limited grounds upon which it can be invoked.[208] While the right itself is not without controversy and has been the subject of intense debate in Europe, the rationale for its existence was correctly underscored in *Google Spain*[209] where the Court held that the right to privacy is greater than the economic interest of the commercial firm and, in some circumstances, the public interest in access to information. Thus, its absence from CDPA leaves a lot to be desired as there are circumstances where an individual's right to privacy will be greater than the public interest of access to information and commercial gain.

The second such right excluded from the Act is the right to data portability. The right allows a data subject to receive their data in a structured, common and machine-readable format. The importance of the right is to give more control over data to the subjects to allow for the free movement of data between providers. At a time when data sharing and reuse of data are becoming more mainstream in the digital economy, the absence of a right to data portability significantly hinders the ability of data subjects to move between service providers. The third right excluded from CDPA is the right to the protection of personal information or data. The Zimbabwean Constitution contains a right to privacy but not a right to the protection of personal information. While there is a relationship between privacy and the protection of personal information, the two rights are distinct.[210]

There is no consensus among scholars regarding what constitutes a right to privacy, but most definitions are framed in terms of information control.[211] Privacy is a 'claim of individuals, groups or institutions to determine when, how and to what extent information about them is communicated to others'.[212] A right to the protection of personal data seems to suffer a similar fate with some scholars arguing that the essence of the fundamental right to the protection of personal data is an elusive concept.[213] However, at its core, a right to protection of personal data enables people to check the accuracy and relevance of data concerning them, how personal data files should be properly set up and managed,

208 GDPR (n 45) art 17.
209 Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317.
210 An examination of the distinction between the two rights is beyond the scope of this work. For a discussion of the difference between the two rights, see M Tzanou 'Data protection as a fundamental right next to privacy? "Reconstructing" a not so new right' (2013) 3 *International Data Privacy Law* 88-99. See also G González Fuster *The emergence of personal data protection as a fundamental right of the EU* (2014).
211 LA Bygrave 'The place of privacy in data protection law' (2001) 24 *University of New South Wales Law Journal* 277.
212 As above.
213 M Brkan 'The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the CJEU's constitutional reasoning' (2019) *German Law Journal* 878.

and legal sanctions for the misuse and abuse of personal data.[214] A right to data protection, therefore, is concerned with 'informational autonomy'.[215]

Despite their differences, the rights to privacy and protection of personal data interact in several ways.[216] In Zimbabwe, section 57 of the Constitution protects the right to privacy. It includes the right not to have possessions searched or seized, premises entered, communications infringed, and health data disclosed without authority. The right to privacy has been interpreted as being the right not to be subjected to the scrutiny of personal life or business.[217] The interpretation was premised on the interpretation of the right to privacy by the South African Constitutional Court in the case of *Gaertner & Others v Minister of Finance & Others*[218] in which it was held that '[t]he right to privacy embraces the right to be free from intrusions and interference by the state and others in one's personal life'.[219]

The Supreme Court of Zimbabwe in *Netone v Econet* interprets the essence of the right to privacy as being informational control. The right to privacy in the Zimbabwean Constitution, therefore, focuses predominantly on informational control. However, there is an element of informational autonomy derived from a reading of section 57(1)(e) of the Constitution, giving people a right not to have their health data disclosed. Nonetheless, informational autonomy is limited to health data. This means that the right to privacy as provided for in the Constitution does not cover informational autonomy, which is the essence of the right to data protection. Thus, the constitutional right to privacy on its own is inadequate to regulate issues of data protection.

Section 47 of the Constitution states that the rights contained in chapter 4 of the Constitution do not preclude the existence of other rights and freedoms that may be recognised or conferred by law, to the extent that they are consistent with the Constitution. CDPA, therefore, ought to have created a separate right to the protection of personal information to complement the constitutional right to privacy. This is because a right to protection of personal information would serve multiple interests potentially extending beyond the traditional concepts of privacy.[220] The view carried by CDPA that the protection of personal information essentially is privacy protection may obscure the realisation of the benefit of data

214 See the explanation of Hondius as to why there was a separate need for protection of personal data that differed from privacy and confidentiality. F Hondius 'A decade of international data protection' (1983) 30 *Netherlands International Law Review* 103-128.
215 Tzanou (n 210) 89.
216 A Rouvroy & Y Poullet 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy' in S Gutwirth and others (eds) *Reinventing data protection*? (2009) 45.
217 *Netone Cellular (Private) Limited & Another v Econet Wireless (Private) Limited & Another* SC 47/18.
218 [2013] ZACC 38; 2014 (1) SA 442 (CC).
219 As above.
220 Bygrave (n 211).

protection to society as a whole and might ultimately hamper advocacy and the development and implementation of stronger data protection laws.

CDPA also lacks remedies for data subjects in the event of a breach. Data subjects, therefore, could use the law of delict to recover damages for data breaches or unlawful data processing causing harm. Whether the law of delict will provide recourse in the event of harm remains to be seen, given the rigidity of Zimbabwean courts in extending the applicability of the common law. The best approach, however, would be for a separate cause of action to be created targeting harm resulting from data breaches. Whether data subjects would succeed is one thing, but the absence of recourse leaves much to be desired.

4.12 Transfer of personal information outside Zimbabwe

CDPA prohibits the transfer of personal information to a third party in a foreign country or an international organisation unless an adequate level of protection is ensured in the country of receipt or recipient international organisation.[221] Adequacy is assessed considering all circumstances surrounding a data transfer operation, namely, the nature of the data; the purpose and duration of the proposed processing; the recipient third country or international organisation and professional rules; and security measures that are complied with within the third country or international organisation.[222] POTRAZ has exclusive authority to determine categories and circumstances in which the transfer of data to countries outside Zimbabwe is unauthorised. When a country has an adequacy decision and POTRAZ has made a list of data that is ineligible to be transferred outside Zimbabwe, data will not be able to leave Zimbabwe.[223] Whether such a provision will be consistent with the provisions of AfCFTA remains to be seen as this is not a standard clause in data protection legislation.

Transfers of data to a country devoid of an adequate level of protection can occur in six circumstances. The first is where the data subject has unambiguously consented.[224] The second is where the transfer is necessary for the performance of a contract between the data subject and the data controller or in the implementation of pre-contractual measures at the request of the data subject.[225] The third is where the transfer is necessary for the conclusion or performance of a contract that is concluded or is to be concluded by the data subject and the data controller.[226] The fourth is where the transfer is necessary on public interest grounds or for the establishment, exercise or defence of legal claims.[227] The fifth

221 CDPA (n 1) sec 28(1).
222 CDPA (n 1) sec 28(2).
223 CDPA (n 1) sec 28(3).
224 CDPA (n 1) sec 29 (1)(a).
225 CDPA (n 1) sec 29(1)(b).
226 CDPA (n 1) sec 29(1)(c).
227 CDPA (n 1) sec 29(1)(d).

is where a transfer is necessary to protect the data subject's vital interests.[228] The sixth is when the transfer is made from a register that is intended to provide information to the public and is open to the public in terms of an Act of Parliament or regulations.[229] There is no obligation of disclosure to the data subject when the controller intends to transfer personal data to a third country or international organisation and whether a decision of adequacy exists. Disclosure would only occur when the data controller seeks the data subjects' consent for such transfer.

4.13 Offences and penalties

CDPA provides for criminal penalties for violations of its provisions. The penalties may be imposed on data controllers, their representatives, agents or assignees when they violate the provisions relating to the processing of sensitive data; when they fail to fulfil duties in terms of section 13;[230] when they are not accountable as prescribed by section 24; when they transfer data outside Zimbabwe, against the provisions of section 28; and when they contravene the security requirements under section 18(4). Once found guilty, the data controller or their representatives will be liable to a fine not exceeding level 11[231] or to imprisonment for a period not exceeding seven years or to both such fine and such imprisonment.[232] The court may also order the seizure of the media containing the data to which the offence relates or the deletion of the data. The computers themselves are not liable for seizure in terms of CDPA.[233]

Objects seized post-conviction must be destroyed, and the data controller shall be liable for the payment of the fines incurred by the agent or assignee. POTRAZ is not authorised to issue penalties or fines for violations of CDPA by data controllers and processors. Prosecution for violation of CDPA will be left to the NPA as violations are criminal offences that attract imprisonment, and it is the constitutional mandate of the NPA to prosecute criminal offences. This limits the enforcement capabilities of POTRAZ. Ideally, POTRAZ should be empowered to issue administrative fines and penalties for violations of CDPA.

228 CDPA (n 1) sec 29(1)(e).
229 CDPA (n 1) sec 29(1)(f).
230 CDPA (n 1) sec 13: 'Duties of data controller: Every data controller or data processor shall ensure that personal information is – (a) processed in accordance with the right to privacy of the data subject; (b) processed lawfully, fairly and in a transparent manner in relation to any data subject; (c) collected for explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes; (d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed; (e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required; (f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay; and kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected.
231 For transgressions classified under level 11, the fine will not exceed US $1 000 in accordance with Statutory Instrument 14A of 2023.
232 CDPA (n 1) sec 33(2).
233 CDPA (n 1) sec 33(3).

These could include powers such as an order to stop processing or an order to delete data that is held by the data controller.

5 Conclusion

CDPA is a significant step towards protecting personal information in Zimbabwe, considering the absence of protection of personal information under common law and customary law. Private entities had no obligations to protect personal information under AIPPA. They are now obliged to protect personal information under CDPA. The protection of personal information is premised on the constitutional right to privacy. While CDPA reflects modern-day data protection law in most of its provisions, it has several weaknesses. These include using privacy as a premise for the protection of personal information rather than an independent right to data protection; the failure to include other data subject rights such as the right to be forgotten, the right to approach the courts for compensation for infringements of CDPA; the DPA lacking power to prescribe administration sanctions; as well as the absence of provisions guaranteeing the independence of the DPA and inadequate provisions on disclosure to data subjects.

CDPA also fails to address its relationship with the CPA, creating room for forum shopping and the possibility for divergent enforcement by two different DPAs. However, some of the weaknesses in CDPA can be rectified through statutory instruments issued in terms of CPDA or through guidance by POTRAZ. The regulations can lay down requirements for data controllers and processors to conduct impact assessments, and implement data protection by design and default. The regulations can also lay down rules on the nature of the right to access, circumstances when consent can be assumed, and requirements for data subjects to be notified of serious data breaches. It is also recommended that CDPA be amended to include other data subject rights such as the right to be forgotten as well as the right to data portability. This should be accompanied by remedies for data subjects when there have been violations of their rights. The supervisory function should be removed from POTRAZ and an independent authority established and given the status of a constitutional commission. These recommendations will act to further strengthen the significant inroads CDPA has made in ushering Zimbabwe into a new age of data protection.

African Journal on Privacy & Data Protection

To cite: S Goliath 'The Protection of Personal Information Act 4 of 2013: Child social media influencers and their right to privacy' (2024) 1
African Journal on Privacy & Data Protection 81-98
https://doi.org/10.29053/ajpdp.v1i1.0005

The Protection of Personal Information Act 4 of 2013: Child social media influencers and their right to privacy

*Stacey Goliath**
LLM Candidate, Private Law Department, University of Stellenbosch, South Africa

Abstract:

'Social media influencing' has developed in recent years. It is the practice of sharing ideas, practices and products on online platforms to influence other users to purchase products or engage in certain practices. This is done in exchange for remuneration from companies or the social media platforms themselves once influencers have a large enough following. A core part of social media influencing is the transparency of the influencer with their audience. To achieve this transparency, many social media influencers share rather personal information to connect with their audience. Children have also started participating in social media influencing. Both regional and South African legal frameworks recognise the child's best interests, and their vulnerability. Since children have begun to occupy an important position as social media influencers, this article provides a South African perspective on the extent to which the Protection of Personal Information Act 4 of 2013 (POPIA) protects the privacy of the child involved. The article specifically considers how the child's privacy right is impacted when participating in social media influencing, and the way in which POPIA interacts

* BA, LLB University of Stellenbosch; staceyg@sun.ac.za. I wish to thank the two anonymous reviewers and the editors for their helpful guidance and contributions. I am grateful to Dr Debbie Horsten for her support and encouragement in the writing of this article.

with such impact. The argument proposed is that the current formulation of POPIA neither specifically provides for nor fully regulates the practice of social media influencing due to the incredibly nuanced nature of the practice. The article further argues that even though POPIA addresses the issues of children's digital privacy generally, it does not extend its scope to the specific circumstances where children are social media influencers. The article ultimately seeks to question whether POPIA recognises and protects the child influencer's privacy rights.

Key words: children's rights; right to privacy; social media influencers; Protection of Personal Information Act 4 of 2013

1 Introduction

There have been significant shifts in South African law to address the changes brought about by technology, and to fulfil the state's legal obligation towards children in this new space. An example of this is the promulgation and coming into effect of the Protection of Personal Information Act 4 of 2013 (POPIA).

POPIA was founded upon the recognition of the section 14 right to privacy as included in the Constitution of the Republic of South Africa, 1996 (Constitution).[1] POPIA recognises that this right includes the right to the protection of information.[2] The legislative text of POPIA provides that its purpose is to implement the right to privacy through the protection of personal information while also balancing other, competing rights and interests.[3] Thus, this article will seek to consider the role POPIA plays in protecting privacy, when the child partakes in the practice of what has become known as 'social media influencing'.

For the purpose of the article, 'social media influencing' should be understood as a form of 'digital marketing' whereby individuals (that is, the social media influencer) advertise products and lifestyle choices on social media platforms using their personal social media accounts. These individuals have built a trusted network of followers who rely on their opinions and support their viewpoints.[4] Influencers will post photographs or videos of themselves encouraging their follower network to buy the product, use the service offered by the company or even make certain decisions.[5] For example, social media influencers were used by political parties and corporations to influence political discourse and

1 Preamble to the Protection of Personal Information Act 4 of 2013 (POPIA).
2 As above.
3 Sec 2 POPIA.
4 K Weerasinghe & C Wijethunga unpublished paper presented at Australasian Conference on Information Systems (2022) 2 4; M de Veirman, L Hudders & MR Nelson 'What is influencer marketing and how does it target children? A review and direction for future research' (2019) 10 *Frontiers of Psychology* 2.
5 Nashville Film Institute 'Social media influencer – Everything you need to know' (nd), https://www.nfi.edu/social-media-influencer/ (accessed 5 December 2023).

voter behaviour.[6] Influencers may be paid by the companies whose products they advertise or by the social media platforms as influencers increase traffic by consumers to these platforms.[7] Incentivisation schemes, such as the TikTok Creator's Fund and YouTube's Partner Programme, are examples of how the social media platforms create income generation opportunities for influencers.[8]

Recently, there has been a global increase in parents including or using their children to generate the content for these purposes.[9] Parents perform an integral role in the creation of this content as children that are of a younger age may not have the ability to create, share or post this content. The type of content posted by these parents of their children may include prank videos,[10] toy reviews[11] or vlogs.[12] Vlogging, for example, is a particularly successful area of participation for children as influencers.[13] The content may also concern issues faced by the child in their personal life.[14] This article will focus on children's participation in influencing, either alongside or under the instruction or guidance of their parent,[15] and how effective POPIA is in protecting such child's privacy. In considering this, the article first provides an overview of the issue to sketch the relevant context. The article will then engage with the effects of social media influencing in relation to the child influencer's right to privacy under South African law. Finally, the article will establish whether, given these effects, POPIA provides sufficient oversight and protection of the child as a social media influencer.

2 Children as social media influencers

Social media influencing and children's involvement therein are not confined to a single social media platform. YouTube, Instagram and, more recently, TikTok are all examples of platforms on which social media influencers, particularly child

6 M Riedl, J Lukito & S Woolley 'Political influencers on social media: An introduction' (2023) *Social Media and Society* 2.

7 M Nouri 'The power of influence: Traditional celebrity v social media influencer' (2018) 32 *Advanced Writing: Pop Culture Intersections* 125.

8 *TikTok*, https://www.tiktok.com/creators/creator-portal/en-us/getting-paid-to-create/creator-fund/, https://support.google.com/youtube/answer/72851?hl=en (accessed 25 February 2023).

9 S Steinberg 'Sharenting: Children's privacy in the age of social media' (2017) 66 *Emory Law Journal* 872.

10 https://www.youtube.com/watch?v=-Zw3mGZGpFA (accessed 14 September 2023).

11 Nashville Film Institute (n 5).

12 S Mariasih & G Tambunan 'Linking privatised large family domestic space with a public audience: An analysis of housewives who are YouTube vloggers' (2020) 28 *Pertanika Social Sciences and Humanities* 588.

13 'Vlogging' refers to the practice of posting short videos on social media platforms. See M Jansen 'Growing up on YouTube – How family vloggers are establishing their children's digital footprints for them' (2017) *Masters of Media* 8.

14 F Latifi 'Chronic illness influencers on TikTok are showing the reality of being sick' *Teen Vogue* 22 September 2022, https://www.teenvogue.com/story/chronic-illness-influencers-on-tiktok-are-showing-the-reality-of-being-sick (accessed 5 December 2023).

15 Jansen (n 14) 8.

influencers, have had a presence.[16] YouTube was one of the earliest platforms used for large-scale social media influencing among families.[17]

Instagram has also been used for the purposes of social media influencing, particularly by companies paying influencers to endorse their brands.[18] An example of this is Kairo Forbes, the daughter of well-known South African performers. Kairo is only seven years old but has a prominent social media presence that has resulted in her being offered marketing deals with large companies such as Cotton on Kids[19] and Roblox.[20]

TikTok, as a more recent platform, has become impressively popular over the last few years and allows for the posting of shorter-form videos.[21] All TikTok users have access to what is known as the 'For your page', which is programmed by a structured algorithm which allows the application to curate content for the users of the platform.[22] This enables the content of influencers to reach many people who would be interested in their content quickly. TikTok, and the other social media platforms, have been used by both those already famous and 'ordinary people' to achieve fame.[23] An example of the latter is the use by parents to post their children for the purposes of social media influencing as a means to generate financial reward. This has been done through the advertising for companies or through the TikTok Creator's Fund that was set up for the purposes of TikTok paying influencers for the content posted by them once a certain level of engagement has been reached.[24] Although the social media platforms mentioned are different in nature, they all provide opportunities for influencers to generate financial reward through the use thereof.

This phenomenon of social media influencing has infiltrated many countries, including countries in the African region. This article focuses on South Africa, which recently has witnessed a growing trend of social media influencing involving children. For instance, Kairo Forbes, daughter of a popular former South African rapper, has over one million followers on Instagram.[25] Another example is Sbahle Mzizi, a young child, who has one million Instagram followers. She has also been

16 As above.
17 Jansen (n 14) 4.
18 S Kay and others 'When less is more: The impact of macro and micro social media influencers' disclosure' (2020) 36 *Journal of Marketing Management* 278.
19 K Forbes 'KairoForbes and CottonOnKids' *Instagram*, https://www.instagram.com/p/ClptaImoTgx/?utm_source=ig_web_copy_link (accessed 6 December 2023).
20 As above.
21 Y Wang 'Humour and camera view on mobile short-form video apps influence user experience and technology-adoption intent, an example of TikTok (*DuoYin*)' (2020) 110 *Computers in Human Behaviour* 1.
22 As above.
23 A Jerslev & M Mortensen 'Celebrity in the social media age: Renegotiating the public and the private' in A Elliot (ed) *Routledge handbook of celebrity studies* (2018) 169.
24 To date TikTok has not publicly provided the criteria to be part of the Creator's Fund.
25 Forbes (n 19).

offered marketing deals by large companies such as Game.[26] These are but two examples of a growing trend on the African continent of social media influencing. Taylor Morrison, a young girl with over 200 000 followers on Instagram, shot to fame after videos of her posted by her mother went 'viral'.[27] She has since been sponsored by well-known brands, including The Crazy Store, Fashion Nova and LOL Surprise South Africa. These are but three examples of a growing trend on the African continent of children being used in social media influencing. This phenomenon has grown so much in the African region that television network Nickelodeon has created a category for Best African Kidfluencer for its annual Kids Choice Awards.[28] This is indicative of the relevance of the issue in South Africa and why it is worth considering. Although reference will also be made to influencers in foreign jurisdictions, this article aims to provide a South African perspective on this issue that is of global relevance. In order to do this, the article first sets out what the child's 'right to privacy' entails and how it is implicated when children are social media influencers. Thereafter, POPIA will be considered on selected grounds to establish the extent to which it addresses the implications of child social media influencing on the child's right to privacy. This will be done in order to conclude whether the protection provided by POPIA may be regarded as adequate in protecting the child influencer's right to privacy.

3 3 Link between social media influencing and the child's right to privacy

3.1 Right to privacy

The inclusion of the right to privacy in the South African Constitution was an important step in cementing the importance of and emphasis on privacy rights in South Africa. Its inclusion in section 14 of the Constitution sets out both general and specific grounds that are protected under the ambit of the right. Importantly, these grounds are not a closed list, and courts are free to interpret to take a more encompassing approach when interpreting this right.[29] The significance of the right to privacy emanates from its blatant disregard and, sometimes, the infringement of the right, under the apartheid regime.[30] Given the above, South

26 S Mzizi 'SbahleMzizi' *Instagram* 6 December 2021, https://www.instagram.com/p/CXJLAXroMKu/?hl=en (accessed 25 February 2023).
27 B Forbes-Hardinge, https://getitmagazine.co.za/highway-berea/blog/2022/04/28/keeping-up-with-taylor/ (accessed 14 September 2023).
28 M Zuma 'Meet the Nickelodeon African Kidfluencer nominees' *Sunday World* 24 March 2022, https://sundayworld.co.za/celebrity-news/entertainment/meet-the-nickelodeon-african-kidfluencer-nominees/ (accessed 28 March 2023).
29 I Currie & J de Waal (eds) *The Bill of Rights handbook* (2013) 302.
30 J Neethling, J Potgieter & A Roos *Neethling on personality rights* (2019) 46.

Africa's constitutional dispensation ushered in a shift towards viewing the privacy right as a fundamental human right.[31]

The Children's Act 38 of 2005 (Children's Act), the piece of South African legislation giving content to the rights of the child, provides in section 6(2)(a) that all matters or proceedings that concern a child should give effect to their rights as enshrined in the Bill of Rights of the Constitution. The right to privacy, as contained in section 14 of the Constitution, is one such right.

The United Nations Convention on the Rights of the Child (CRC) grants the child a right to privacy as contained in article 16 thereof. During the drafting of the CRC, it was found that recognising the child's privacy means recognising their personhood and status as right bearers.[32] Hence, article 16 also applies to governments as well as individuals such as children's parents. Governments are tasked with protecting the privacy of the child and may not unduly infringe thereon.[33] CRC was domesticated into South African law in section 28 of the Constitution, which provides a detailed provision of children's rights, drawing inspiration from CRC.[34] Section 231 of the Constitution regulates international agreements and their status in South African law. The provision requires that an international agreement becomes law in the Republic once it is domesticated into South African law.[35]

Other international instruments[36] also recognise the right to privacy. However, the Universal Declaration of Human Rights (Universal Declaration) does not automatically create legal obligations on states, unless it is given the force of *ius cogens*.[37] This shows a very prominent position of the right within the international law framework. This adds another level of importance to the right in the South African context. Section 233 of the Constitution also provides for the application of international law, and requires that the interpretation of domestic law provisions should be aligned with international law.

Beyond international law, there also is a regional law obligation on South Africa to protect the right to privacy. On a child law level, the African Charter on the Rights and Welfare of the Child (African Children's Charter in article 10 recognises that the child has a right to privacy that should not be interfered with, excluding circumstances where caregivers need to exercise reasonable supervision over the child. As is the case with CRC, the courts have held that the African Children's Charter inspired the drafting of section 28 as many

31 Neethling and others (n 30) 6-48.
32 S Detrick *A commentary on the United Nations Convention on the Rights of the Child* (1999) 270.
33 As above.
34 J Tobin 'Increasingly seen and heard: The constitutional recognition of children's rights' (2005) 21 *South African Journal on Human Rights* 86-126.
35 TW Bennett & J Strug *Introduction to international law* (2013) 27.
36 International Covenant on Civil and Political Rights art 17.
37 Bennett & Strug (n 35) 27.

principles contained in section 28 reflect the text of the Children's Charter. This domestication indicates the commitment of South Africa to realising the rights provided in these children's rights conventions.[38]

In addition to privacy, generally, the African region has also recognised the importance of the protection of data privacy as part of the right to privacy.[39] On 27 June 2014 the African Union (AU) adopted the Convention on Cybersecurity and Personal Data Protection (Malabo Convention)[40] which had the objective of protecting data privacy. It provided that state parties should commit to adopting legal frameworks that strengthen the right to privacy, particularly where it concerns personal data. It also emphasises the fact that violations of privacy should be punished.[41] On 9 May 2018 the Personal Data Protection Guidelines for Africa (DPA) were drafted. However, only 14 member states have to date ratified the Convention, of which South Africa is not one.[42]

Interestingly, the African Charter on Human and Peoples' Rights' (African Charter) does not protect the right to privacy. However, its drafting in 1981 preceded the digital age in which the protection of privacy became more important.[43] Nevertheless, the right to privacy is still protected by African regional instruments and guidelines, and 52 African states have included the right in their constitutions.[44]

This inclusion in child law-specific human rights instruments as well as human rights instruments generally reflects the importance of the right in human rights discourse. It is not a right that is only granted to a sub-set of people but rather is present across various different types of instruments. It therefore is clear that the right to privacy is important for several reasons. This article will now turn to consider how the child's right to privacy is implicated when a child is a social media influencer.

3.2 Social media influencing and the right to privacy

The Court[45] has held that the right to privacy is implicated when a person 'has the ability to decide what he or she wishes to disclose to the public and the expectation that such a decision will be respected is reasonable'.[46] The right to

38 *Director of Public Prosecutions, Transvaal v Minister for Justice and Constitutional Development* 2009 (4) SA 222 (CC) para 76.
39 A Singh & M Power 'The privacy awakening: The urgent need to harmonise the right to privacy in Africa' (2019) 3 *African Human Rights Yearbook* 207.
40 As above.
41 Art 8(1) African Union Convention on Cyber Security and Personal Data Protection.
42 African Union 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection' (2023).
43 Singh & Power (n 39) 218.
44 Singh & Power (n 39) 203.
45 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd: In re Hyundai Motor Distributors (Pty) Ltd v Smit NO* 2001 (1) SA 545 (CC) para 16.
46 As above.

privacy, therefore, functions to protect the information of an individual should they not wish to disclose this information to the public.[47] The information in question may also take the form of data. Data privacy is recognised as a form of 'informational privacy'.[48] In 2009 the South African Law Reform Commission (SALRC) recognised that the growth of technology, particularly computer databases and electronic networks, necessitated data protection legislation similar to the European Union Data Directive.[49] This recognition by the SALRC reflected a responsive attitude by the law to the changing circumstances in society. In 2021 POPIA came into effect as one of the consequences of this report.

The right to privacy is not only important, but is also *relevant* in this case for the following reasons: Private information may be defined as the 'sum total of information or facts relating to an individual in his condition of seclusion and which are thus excluded from the knowledge of outsiders'.[50] Social media influencing may involve the sharing of personal information, or information to which outsiders usually are not privy, as many influencers achieve success by publishing content that is highly curated, often involving aspects of the influencer's personal life.[51] This sharing of information allows the audience to feel closer to the influencer, which then further increases viewership and, by extension, increases popularity.[52] Social media users, who are not already established celebrities and often do not have a specialisation such as acting or performing, rely on 'developments in their personal lives to connect with their followers and establish their self-branding'.[53] In this context, this would mean that the basis of their platform is the sharing of personal and intimate details about the child.[54] For example, this information may include anything from the type of hobbies someone enjoys to information about a influencers' medical details, diagnoses or filming of actual medical episodes[55] or, particularly in the family influencing arena, videos of neurodivergent children becoming overstimulated.[56] Because of the uniqueness of their content, there is an increased public interest in this very specialised content which increases the following of the influencer.[57] Companies are also attracted to these influencers as the range of product placement increases, particularly in countries such as the United States of America where pharmaceutical companies are highly-commercialised entities.[58] Some influencers

47 As above.
48 Currie & De Waal (n 29) 303.
49 As above.
50 Neethling and others (n 30) 46-48.
51 C Abidin "Aren't these just young, rich women doing vain things online? Influencer selfies as subversive frivolity' (2016) 2 *Social Media and Society* 3.
52 As above.
53 As above.
54 Latifi (n 14).
55 I Garcia *TikTok* 19 September 2023, https://www.tiktok.com/@ivette_boricuanena/video/7280642354950802730 (accessed 5 December 2023).
56 C Bonnello 'Ten vital reasons to never, ever share an autism meltdown video' 17 August 2020, https://autisticnotweird.com/meltdown-videos/ (accessed 5 December 2023).
57 Kay and others (n 18) 278.
58 FD Ledley and others 'Profitability of large pharmaceutical companies compared with other large public companies' (2020) 323 *Journal of the American Medical Association* 835.

and even established celebrities have falsely told their supporters that they or their children are suffering from challenging or rare medical issues, through the generation of such content depicting this, with such videos reaching millions of viewers.[59] This indicates how receptive the public is to this kind of content.

Additionally, one cannot control the identity of or size of the audience engaging with their content.[60] Once the content is shared, and the audience has grown, there is a lack of control over what the audience will do with the content, or whether and how they will further distribute such content.[61] As the content is reshared, audience sizes increase.[62] TikTok, for example, frequently allows older content to resurface, with content becoming popular years after it was first posted.[63]

However, in South African law, for information to be regarded as private, the subject must subjectively expect or want the information to be treated as private.[64] At this vantage point one cannot yet draw conclusions as to what individual social media influencers expected or wanted. This, however, does warrant careful consideration of whether this content should be shared at all, particularly because of the vulnerability of children and how their interests are to be protected by those tasked with doing so.[65] This subjective expectation must, however, be objectively reasonable.[66]

When determining whether the subjective expectation of non-disclosure is objectively reasonable, the court is more likely to engage in such consideration where the expectation concerns the 'inner sanctum' of a person.[67] For instance, in *NM v Smith*[68] it was found that the disclosure of medical information without full and informed consent amounts to an infringement of privacy because medical information forms part of this 'inner sanctum'.[69] In this analysis of social media influencing, it will become clear that similar types of information are disclosed. This could potentially amount to sharing of information that objectively is part of the inner sanctum of the child, that should be appropriately regulated.

59 C Young 'Family vloggers are using cancer as clickbait and coaching tears for views' *Betches* 10 September 2021, https://betches.com/family-vloggers-are-using-cancer-as-clickbait-and-coaching-tears-for-views/ (accessed 5 December 2023).
60 T de Beer & E Sadleir *Don't film yourself having sex and other legal advice for the age of social media* (2014) 154.
61 As above.
62 As above.
63 C Ahlgrim & T Tyson 'How TikTok revives old songs and turns them into new hits' *Business Insider* 11 April 2023, https://www.insider.com/popular-tiktok-songs-from-past-decades-trending-now-2023-4 (accessed 5 December 2023); Wang (n 21) 9.
64 Currie & De Waal (n 29) 302.
65 R Songca 'Evaluation of children's rights in South African law: The dawn of an emerging approach to children's rights' (2011) 44 *Comparative and International Law Journal of Southern Africa* 344.
66 *Bernstein v Bester* 1996 (2) SA 751 (CC) para 75.
67 *Bernstein v Bester* (n 66) para 28.
68 *NM v Smith* 2007 (5) SA 250 (CC) para 40.
69 As above.

From the above it is clear that privacy most certainly is implicated in the practice of social media influencing involving children. Children are not shielded from the impacts thereof and careful consideration of this issue is warranted. Given the fact that POPIA is the most specific piece of legislation governing data protection in South Africa today, I will consider its role in this specific context.

4 Child influencers' rights under POPIA

In order to assess whether POPIA appropriately responds to the implication of the child influencer's privacy, this article will engage POPIA on three grounds, namely, its scope, the consent clause involving the processing of children's personal information and relief mechanisms that are available.

4.1 Scope of POPIA

In order for POPIA to apply, it requires the information in question to qualify as personal information, and it must pertain to a data subject.[70] Section 1 of POPIA provides that personal information can take the form of various classes of information. These may range from information about a data subject's biographical information, such as their name or age, to their medical or criminal history. It is the author's submission that content posted by social media influencers can and has been included in many of the aforementioned categories – especially in circumstances in which the foundation upon which the platform of the influencer is built is the very defining characteristic of the child.

For instance, an example of a type of social media influencing involving children is where parents of medically-complex or particularly[71] vulnerable children document their experiences with their children's illnesses or vulnerabilities. This is done on various social media platforms and has presented the same monetisation opportunities.[72] The entire social media account is then focused on the child's everyday lived experience with their conditions.[73] This is but one example of how the content posted in the process of social media influencing can fall into the category of 'personal information', which would make POPIA applicable.

The aforementioned examples by no means are an exhaustive list of examples of information that can be shared in the process of social media influencing where children are involved. However, what the examples do indicate is that this kind of information is very often divulged. Therefore, the content shared

70 Sec 1 of POPIA regards a data subject to be a 'natural or juristic person'.
71 The use of the word in this context refers to the children in question having certain characteristics or aspects of their personhood that make them even more vulnerable than they would be only as a result of their minority. See J Heaton *The South African law of persons* (2017) 79.
72 Latifi (n 14).
73 As above.

of these child influencers can qualify as 'personal information' under POPIA. The type of personal information in question depends on the specific influencer, however. It is also true that not all influencers intend to share this information. However, POPIA does not distinguish between intentional or accidental sharing of personal information. Thus, whether or not the information was intentionally shared, it can nevertheless still be shared indirectly through references to the information or background.

Even if one were to argue that personal information does not have to be shared to become an influencer, a glance at the platforms of the most successful child influencers previously discussed indicates that this is the kind of information that is usually divulged in order to establish and expand the platforms. The sharing of personal information has also been recognised as part of the success in establishing the para-social relationship with the followers.[74] The qualification of this content as personal information under POPIA means that, on this ground, POPIA has application. The scope of POPIA is not only determined by the type of content, but also by the *objective* of the influencer posting the content.

The objective requirement of POPIA is important because its scope excludes 'the processing of personal data' for household or personal objectives.[75] This means that POPIA would not apply in circumstances where, for example, a list of contact numbers of friends is kept in a family home for family use.[76] In circumstances such as these, the controller of the personal information would not be defined as a 'data controller' and the obligations in terms of POPIA would not apply to this data, even if the data is regarded as 'personal information'. Put simply, if the personal information is used for purely personal reasons, then it is not personal information subject to the protection provided by POPIA.

However, it does become difficult to draw this distinction in the age of social media, especially where personal information as defined in POPIA is published on social media platforms, including Facebook and Instagram.[77] This difficulty is no clearer than in the case of social media influencing where personal information is shared.[78] Where then does one draw the line to determine whether such information falls within the regulatory ambit of POPIA? This lack of clarity is compounded by the fact that sharing content of children on social media networks can also be done for the sole purpose of keeping family and friends up to date with the child's life. This has commonly been referred to as 'sharenting'.[79]

74 Nouri (n 7) 9.
75 Sec 6(a) POPIA.
76 DP van der Merwe and others *Information and communications technology law* (2021) 439.
77 As above.
78 Nouri (n 7) 9.
79 'Sharenting' is 'the habitual use of social media to share news and images of one's children'. See A Fox & M Hoy 'Smart devices, smart decisions? Implications of parents' sharenting for children's online privacy: An investigation of mothers' (2019) 38 *Journal of Public Policy and Marketing* 432.

Examples of this would be sharing photo albums of the child's milestones, such as birthdays or achievements, on platforms such as Facebook.

However, there is a fundamental difference between social media influencing involving children and sharenting. This difference lies in the fact that influencers are remunerated for the content they post. It no longer solely involves sharing updates about the child with loved ones, but rather about sharing with the rest of the world and reaping the financial reward thereof. This means that there is a clear commercial gain or objective linked to child influencers, which takes it far beyond the personal dimension. On this basis, it may be argued that the scope of POPIA indeed regulates child influencers due to its commercial dimension and the fact that it goes beyond the personal objectives exclusion from the scope.

Another crucial consideration when it comes to child influencers and their relationship with POPIA is the consent clause that is contained within the Act. The author will now consider how POPIA formulates this clause and evaluate the efficacy thereof in protecting the child influencer and their right to privacy.

4.2 Consent to post content to social media platforms: Section 35(a) of POPIA

Section 35 of POPIA provides a 'general prohibition' on the processing of children's[80] personal information. It more specifically provides a prohibition on the processing the personal information of children, unless there is 'prior consent of a competent person'. Although section 35 of POPIA provides other circumstances in which such personal information may be processed, this article will only focus on section 35(a) due to the relevance of the provision to the scope of this article.

In order to properly establish the extent to which section 35(a) of POPIA protects the child influencer's privacy, one needs to carefully consider the formulation of the general prohibition and related consent clause, and how it operates. Thus, the article now turns to the operation of 'prior consent' and 'competent person' and what this means for the child influencer's right to privacy.

POPIA provides the definition for 'consent' in section 1 as 'any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information'. Such consent thus is not required to take any specific form such as being exclusively written or verbal. The requirement further states that this consent must be given by a 'competent person'. POPIA then defines 'competent person' as 'any person who is legally competent to

80 POPIA defines a child in sec 1 as 'a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself'.

consent to any action or decision being taken in respect of any matter concerning a child'.

The first and, arguably, most obvious, protective function that this section serves is that it introduces an additional limitation to the sharing of personal information of children above and beyond the general limitations placed on the processing of personal information.[81] It introduces another hurdle that must be overcome before the content of the child may be posted. Consent clauses are not uncommon in legislation regulating issues concerning children. This is because children have a limited capacity to act, and clauses such as these aim to protect children from the immaturity of their own judgment.[82] For instance, section 129 of the Children's Act gives children older than 12 years of age the right to consent to a medical operation provided that they are of sufficient maturity to do so, and duly assisted by their parents or guardians. Children under 12 thus may not themselves provide consent, and will require their parents or guardians to do so on their behalf.

This requirement of consent in and of itself protects the child's privacy by recognising the child's minority status and what this means for their level of vulnerability acting as a factor that influences their ability to make decisions for themselves. However, I argue that the most contentious area of the protective nature of this clause is that it is a competent person that must provide this prior consent, particularly in circumstances where, due to a child's limited capacity, they do not have the ability to consent for themselves.[83] Section 18(3)(c) of the Children's Act provides that a parent or other person that acts as a guardian for the child must provide consent where this is required by law and the child is unable to provide such consent for themselves. This then gives the parent the power to grant this prior consent in terms of section 35 of POPIA. The parent then is inadvertently providing this prior consent for themselves as social media influencing that involves children with limited capacity relies on the parents to help create, share and promote the social media content in question. The question then arises as to what this means for the child's right to privacy.

A legal conundrum is created whereby those tasked with granting consent as a protection mechanism are the same persons to whom this consent must be granted. How then does consent effectively function as a protective mechanism? Parents are heavily incentivised to post the content of their children because of the financial reward and opportunities that may stem from social media influencing, which could be argued to influence their judgment in these circumstances.[84] This financial reward may even be used to provide for the child and positively

81 D Donnelly 'Privacy by design' in the EU General Data Protection Regulation: A new privacy standard or the emperor's new clothes?' (2022) 139 *South African Law Journal* 559.
82 Heaton (n 71) 79; L Schäfer *Child law in South Africa: Domestic and international perspectives* (2011) 11-16.
83 As above.
84 Kay and others (n 18) 278.

change their lives in a material sense.[85] Although section 35 of POPIA protects the child from any other person posting this content, it does not protect the child from the *parent*. Even if parents provide this consent, it does not mean that the consequences of social media influencing, as previously discussed in this article, will simply disappear or lessen. The child's personal and intimate details will still be exposed to very large audiences. This will still implicate their privacy. This is true even where parents grant themselves this consent without intending these negative consequences.

Although parents are tasked with protecting the best interests of their children,[86] it does not necessarily follow that what they think is the best decision for the child actually is the best decision when taking into account all relevant consequences.[87] This is no clearer than when considering that these children who are influencers, will one day become adults with full capacities. This then raises the question of whether POPIA properly provides for this. In determining this, the article will consider whether the 'evolving capacities of the child' are adequately recognised and given effect to by POPIA.

In the case of *S v M*[88] the Court found that children are not mere extensions of their parents and are persons before the law.[89] Being a person before the law means that children have certain rights and capacities within the existing legal frameworks.[90] Liebenberg argues that this recognition is crucial to ensure that children benefit from and are protected by their socio-economic rights.[91] A child's personhood is not reduced by their minority status, even if they primarily exist within a family structure in which this status is emphasised.[92] A balance needs to be struck between the child's autonomy as a full rights bearer, and their need to be protected given their vulnerability that is created by their minority status.[93] The capacity of the child also is not static in nature, but develops, changes and expands as the child matures. Accordingly, a consideration of the child's rights must be done with the child's evolving capacities in mind.[94] Under South African law, this recognition of the 'evolving capacities of the child' also includes the right of the child to participate in matters that concern or affect them.[95] The importance of participation in South African jurisprudence will first be engaged as it is an integral part of the 'evolving capacities of the child'. Participation can

85 Nouri (n 7) 1.
86 M Couzens 'The best interests of the child and the Constitutional Court' (2019) 9 *Constitutional Court Review* 374.
87 M Newbould 'When parents choose gender: Intersex, children, and the law' (2016) 24 *Medical Law Review* 478.
88 *S v M* 2008 (3) SA 232 (CC) paras 18-19.
89 *S v M* (n 88) para 18.
90 *Teddy Bear Clinic for Abused Children & Another v Minister of Justice and Constitutional Development & Another* 2014 (2) SA 168 (CC) para 52.
91 S Liebenberg *Socio-economic rights adjudication under a transformative constitution* (2010) 230.
92 As above.
93 Currie & De Waal (n 29*)* 601.
94 As above.
95 S Varadan 'The principle of the evolving capacities under the UN Convention on the Rights of the Child' (2019) 27 *International Journal of Children's Rights* 307.

be understood as the 'substantial engagement of people in decisions that affect their lives'.[96]

The Court[97] has recognised the centrality and importance of participation in the constitutional democracy.[98] Given that South Africa has a history of excluding certain groups from participating in the political and social spheres,[99] furthering the access to participation by these excluded or vulnerable groups is an important part of the South African legal system.[100] Children have been recognised as one such vulnerable group.[101] Section 10 of the Children's Act grants children a participation right, which involves the right to participate age-appropriately in matters that concern them, with due consideration given to their views and assistance by a competent person if they lack the capacity to participate independently.

CRC also recognises that the child has a 'right to be heard'.[102] Because children have limited capacity,[103] the Convention also recognises the weight given to this right to be heard and takes the child's age and maturity into account.[104] Specifically, article 5 of CRC refers to the evolving capacities and requires that it be taken into account when adjudicating matters concerning children. This is done to recognise and give effect to the fact that children's capacities change with age: the older the child is, the broader their right to participation. These articles show that the child's autonomy is not only important as it recognises them as a right bearer, but also because it gives them a right to participate that is suitable to that specific child at their specific stage of development.[105]

On a regional law level, the African Children's Charter also recognises the importance of the participation of the child. Specifically, articles 7 and 4(2) when read together provide that a child's right to participate and express their views in matters that concern them apply to 'all matters', not only matters of a judicial nature. Additionally, the provisions recognise that a child who 'is capable' has the right to participate in this way.[106] The consent mechanism as provided for in POPIA should ideally operate in a way that recognises the child's evolving capacities. It should not simply be a mechanism that gives the parents a veto over the child's views, or one that entirely disregards the limited nature of the child's

96 S Liebenberg 'The participatory democratic turn in South Africa's social rights jurisprudence' in S Liebenberg *The future of economic and social rights* (2019) 193.
97 *Mashavha v President of the Republic of South Africa* 2005 (2) SA 476 (CC) para 20.
98 As above.
99 Liebenberg (n 96) 194.
100 As above.
101 Songca (n 65) 344.
102 Varadan (n 95) 307.
103 As above.
104 United Nations Committee on the Rights of the Child General Comment 12 'The Right of the Child to be Heard' (2009) CRC/C/GC/12/ para 20.
105 As above.
106 Arts 7 & 4(2) African Children's Committee.

capacity. A few key issues in the current context of child influencers' privacy and POPIA can be identified and will be considered below.

Children who participate in influencing range in age with some children partaking in the practice throughout their entire childhood.[107] This child will not have the same capacity throughout their whole childhood, and recognising that their capacities evolve as they become older is important to acknowledge as an approach suitable for a younger child, such as that a toddler may not suit an older one, such as an adolescent. Given these evolving capacities, a regulatory framework such as POPIA's prior consent mechanism needs to appropriately provide for both scenarios. In its current formulation, the content of the child may be posted should a 'competent person' provide the necessary consent. It neither provides for a participation process that can involve the child, nor does it acknowledge the nuances of a child's capacity that is evolving and nuanced.

Such acknowledgment is especially necessary and important as a feature of the internet is the ability to access information that is not only recent, but also enables the access of and engagement with content that is less recent.[108] This also means that content posted by influencers is able to resurface many years after it was first shared. For instance, there are examples of influencers being impacted by racist tweets that they made years before they became well-known.[109] These tweets, in many cases, have impacted the influencer's earning potential as many brands have dissociated themselves from the influencer because of the effect that the content has on the brand image.[110] Although neither a South African, nor even African example, it is indicative of the potential consequences for these children. What does this mean for the child who is placed before the world by their parents for the purposes of being an influencer? The impact of this is that content shared by parents of their children in the practice of influencing can persist beyond childhood and can impact the child well into adulthood. This remains true even if the content is deleted, or if the child stops participating in the practice of social media influencing at any stage.

It is the author's submission that the POPIA prior consent mechanism does not adequately provide for the child's evolving capacities through recognising their right to participate, nor does it acknowledge that the child influencer will one day reach adulthood and may have different opinions, feelings and views on their exposure.

107 General Comment 12 (n 104) para 20.
108 De Beer & Sadleir (n 60) 154.
109 Wang (n 20) 9.
110 R Reyes 'Influencer Lunden Stallings apologises during honeymoon amid backlash to resurfaced racist tweets: Utterly disgusted and ashamed' *New York Post* 4 October 2023, https://nypost.com/2023/10/04/influencer-lunden-stallings-apologizes-over-resurfaced-racist-tweets/ (accessed 5 December 2023).

The closest example of what could happen to child influencers is considering child actors who reached adulthood and expressed regret at being thus exposed at such a young age.[111] Child actors form part of a much more regulated industry but have still been impacted into adulthood by decisions made by their parents to expose them to the performing arts.[112] What would this then mean for the child influencer, who partakes in a far less regulated industry, in the years to come? This is an important oversight to recognise as permanent consequences of this nature require far more complex regulation and participation by the child than simple consent by the parent.[113]

Even though POPIA places some hurdles and limitations on children's involvement in social media influencing with regard to the general prohibition and associated consent requirement, it does not appear as if the current formulation and the effect thereof by any means are sufficient for the reality of the technological age.

4.3 Relief provided by POPIA

The adequacy of the relief provided for POPIA will now be considered. This will be done in order to assess whether the child will even be able to do anything about this content should they not agree with it being shared to begin with, or no longer wish it to be available to the public at a later stage.

Section 74 of POPIA is the regulating section with regard to any complaints raised in relation to the sharing of personal information. The section enables an aggrieved person[114] to submit a complaint to the regulator[115] should there be interference with the protection of their personal information. POPIA defines interference in section 73 as 'any breach of the conditions for the lawful processing of personal information as referred to in chapter 3'. This would include the regulating provisions of the personal information of children as contained in Part C of chapter 3 of POPIA. The effect hereof is that if the child, or later adult, is not satisfied with the posting of the content or the way in which consent was obtained, they may approach the regulator in this regard. Sections 75 to 99 of POPIA set out the procedure in terms of which these complaints may be brought and appealed. In summary, these complaints must be brought by the data subject – in this instance the child – or whoever acts as an authorised representative in proceedings of this nature. The process involves various administrative steps that – if the child cannot take these on their own – need to be taken by the parent. This again introduces a potential problem in this case as parents may not want

111 L Abascal 'This new film deep dives into Mary-Kate and Ashley's cultural legacy' *Dazed* 30 June 2022, https://www.dazeddigital.com/fashion/article/56450/1/mary-kate-ashley-olsen-twins-sisters-fame-film-zara-meerza-wetransfer-wepresent (accessed 30 March 2023).
112 As above.
113 Newbould (n 87) 478.
114 Sec 1 of POPIA defines person as 'a natural or juristic person'.
115 Sec 74 POPIA.

to remove the content. The best interests of the child principle would demand such removal, but getting to this end would not be easy for a child, particularly where the child does not have the means to do so themselves. Additionally, even if the child were able to approach the regulator and lodge this complaint, deleting the content will not mean destroying the content, and the effects of this content remaining in the public domain indefinitely, as previously discussed, may persist.

5 Conclusions and recommendations

It has been submitted that the relevant sections of POPIA as analysed above are not sufficient to deal with the protection of personal information of child social media influencers. Social media influencing, particularly where children are involved, is a very complex issue. POPIA's relief mechanisms, while theoretically available, arguably are unlikely to be practically possible for children to make use of, or even in instances where children do make use of them, successful. Given this, it cannot be regarded as adequate to respond to this changing landscape. While POPIA does place certain hurdles in place to deal with the processing of children's personal information when considering its scope, general prohibition clause and relief available, it is the author's argument that these are not sufficient in their current formulation. More effective regulation of child influencers is required in order to address these deficits, and appropriately provide for the child's rights in the short and long term. The internet and its influence are growing quickly and constantly. The law needs to keep up with these developments and provide appropriate and effective regulation where this may be necessary; a regulation that POPIA does not provide, but a regulation that is desperately needed.

African Journal on Privacy & Data Protection

To cite: AE Akintayo 'Trends and implications of Nigerian courts' jurisprudence on privacy and data protection: Lessons from comparative foreign jurisprudence' (2024) 1
African Journal on Privacy & Data Protection 99-118
https://doi.org/10.29053/ajpdp.v1i1.0006

Trends and implications of Nigerian courts' jurisprudence on privacy and data protection: Lessons from comparative foreign jurisprudence

*Akinola E Akintayo**
Senior Lecturer and Legal Consultant, Department of Public Law, Faculty of Law, University of Lagos, Lagos – Nigeria

Abstract:

The world is in a data-driven era. From telecommunication to retail, to health care, to banking, to insurance, security services, and so forth, industries and governments are using data to drive business and governmental functions. There is a need, therefore, to effectively regulate data processing in ways that both foster innovation and protect fundamental human rights, especially the right to privacy. The roles and place of courts in the endeavour, however, cannot be overemphasised. Studies show that even in jurisdictions with expansive data protection frameworks, courts are still needed to clarify the law and effectively protect and advance fundamental human rights, including the right to privacy, in the face of ever-expanding technology. Furthermore, the pace of contemporary technology

* LLB (Lagos), LLM (Pretoria), LLD BL (Pretoria); (akinat2002@yahoo.com. An extract of this article was published on a blog: https://thenigerialawyer.com/nigerian-courts-jurisprudence-on-privacy-and-data-protection-and-its-implications-for-freedom-and-autonomy-lessons-from-comparative-foreign-jurisprudence/, earlier in 2023 to enlighten the general public. My gratitude goes to the anonymous reviewers of the *African Journal on Privacy and Data Protection* whose incisive comments and suggestions added notable value to the article.

development is such that questions are already being asked as to whether data protection is not gradually becoming outdated and obsolete. Consequently, a proactive and progressive judiciary is required to ensure that technological development does not leave the law too far behind. Adequate knowledge and awareness of technology-driven development and conceptualisation of the right to privacy is necessary for the courts to effectively perform these critical roles. This brings to the fore the need to articulate the changing paradigm of the right to privacy in the data-driven era and its nexus with effective regulation of data processing (data protection) in the digital age. This article adopts a comparative and doctrinal research methodologies to interrogate and analyse the trends in the Nigerian privacy and data protection case law; it examines their defects, identifies best practices and learning points for Nigerian courts from comparative foreign jurisprudence as well as highlights right to privacy enhancing provisions of the new Nigeria Data Protection Act 2023 for a nuanced and more robust approaches to privacy and data protection adjudication in Nigeria.

Key words: right to privacy; data protection; Nigerian courts' jurisprudence; emerging technologies; Nigeria Data Protection Act 2023

1 Introduction

The world is in a data-driven era. From telecommunication to retail, to health care, to banking, to insurance and security services, and so forth,; industries and governments are using data to drive business and governmental functions.[1] Thus, the need to effectively regulate data processing in ways that both foster innovation and protect human rights, especially the right to privacy, has never become more important. The roles and place of the courts in this endeavour cannot be gainsaid. First, studies reveal that even in jurisdictions with expansive data protection frameworks, courts are still needed to effectively protect and advance individuals' right to privacy in the face of ever-expanding technology. This is more so the case in Nigeria where the Nigeria Data Protection Act 2023, the substantive framework for the regulation of data processing in the country, has just been passed. Second, the pace of contemporary technological development is such that questions are already being asked as to whether data protection is not already becoming outdated and obsolete.[2] This fact makes appropriate and effective privacy regime and enforcement central to citizens' well-being and freedoms in the face of ever-expanding technologies.

However, a proactive and progressive judiciary is a prerequisite to ensuring that technological developments do not leave the law too far behind. Adequate knowledge and awareness of technology-driven development and

1 W Kim and others 'A taxonomy of dirty data' (2003) 7 *Data Mining and Knowledge Discovery* 81-82.

2 D Hallinan and others 'Neurodata and neuroprivacy: Data protection outdated?' (2014) 12 *Surveillance and Society* 55.

conceptualisation of privacy is necessary for the courts to be able to perform these critical roles. There is a need, therefore, to articulate the changing paradigm of the right to privacy in the data-driven era and draw an appropriate nexus between privacy and regulation of data processing (data protection) through the correct conceptualisation of the right to privacy in the digital age.

Two schools of thought are discernible in the judicial conceptualisation of the right to privacy in Nigeria from the academic literature and case law. The first school of thought maintains a clear distinction between privacy and data protection, while the second maintains that data protection is part of and cognisable under the right to privacy.[3] Thus, while a few of the courts' decisions affirm the connection between privacy and data protection, a preponderance number of the cases disavow such connection with the attendant conflicts in the decisions of the courts at the High Court and Court of Appeal levels. This necessitates the articulation of the changing paradigm of the right to privacy in the data-driven era and the charting of the appropriate course for Nigerian courts in the resolution of the conflicting jurisprudence of the courts on privacy and data protection. In doing this, insights will be drawn from comparative foreign jurisprudence in the area of privacy and data protection to identify best practices and learning points for Nigerian courts.

To achieve the above objectives, this article is divided into five parts. Part 1 is this introduction. Part 2 discusses the changing paradigm of the right to privacy in comparative foreign jurisprudence. Part 3 analyses Nigerian case law on privacy and data protection to highlight current trends, identify gaps and discuss the implications of the decisions on fundamental rights and freedoms of citizens. Part 4 identifies pertinent features of comparative foreign jurisprudence and learning points for Nigerian courts. Part 5 concludes the article.

2 Changing paradigm of privacy in comparative foreign jurisprudence

This part discusses the changing perspectives of the right to privacy in light of emerging technologies in comparative foreign jurisprudence below.

Under comparative foreign laws, the changing paradigm of privacy driven by changing technologies is most noticeable in Europe where early developments and changes in the law were first recorded. This started with the article 8 privacy provisions of the European Convention on Human Rights adopted in 1950 (European Convention) and culminated in the watershed European Union (EU) law on personal data protection – the European Union General Data Protection

3 O Babalola 'Privacy versus data protection debate in Nigeria: The two schools of thought' 31 January 2021, https://thenigerialawyer.com/privacy-versus-data-protection-debate-in-nigeria-the-two-schools-of-thought/ (accessed 7 August 2022).

Regulation (GDPR) adopted by the European Union Parliament and European Council in April 2016. Long before GDPR, however, the European Court of Human Rights (European Court) has been using the right to privacy provisions of article 8(1) of the European Convention to engage the rapid evolution and development of information and communications technology (ICT) technologies within the EU. This has given rise to a robust and extensive privacy and data protection jurisprudence of the Court.

The first case analysed by the Court in this regard is *Leander v Sweden*.[4] The Court in this case held that the storing and release of the applicant's personal information in the secret police register without giving him the opportunity to refute the information violated his right to respect of private life under article 8(1) of the European Convention. The Court, however, concluded that the restriction in this particular case was necessary and justifiable in a democratic society.

Data protection has also been held by the Court to be a fundamental part of the privacy provisions of article 8(1) of the European Convention. This is reiterated by the Court in *Z v Finland* as follows: 'In this connection, the Court will take into account that the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention (art 8).'[5] In its elaboration of the scope of personal data, the Court relied on Convention 108 of the Council of Europe that defines personal data as 'any information relating to an identified or identifiable individual ("data subject")'.[6] Thus, information directly identifying a person, such as names and surnames,[7] as well as information indirectly identifying a person, such as the recording of voice samples,[8] internet protocol addresses,[9] banking details,[10] and so forth, has been held to be within the ambit of personal data. Article 8 of the European Convention also covers or protects not only natural persons but also applies to artificial entities where the privacy of their homes or correspondence is deemed to have been violated.[11]

Activities or actions that will implicate data protection or qualify as data processing have been interpreted by the courts to include the 'storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination' in terms of the meaning of data processing in Convention 108'.[12] Thus, the collection and storage of monitoring data collected via global positioning system (GPS) and other surveillance

4 Application 9248/81.
5 Application 22009/93 para 95.
6 Art 2(a) Convention108 of the Council of Europe.
7 *Mentzen v Latvia* Application 71074/01 (December 2004).
8 *PG and JH v The United Kingdom* Application 44787/98 (September 2001).
9 *Benedik v Slovenia* Application 62357/14 (July 2018).
10 *MN & Others v San Marino* Application *28005/12 (*0ctober 2015).
11 *Liberty & Others v The United Kingdom* Application 58243/00 (2008).
12 Art 2(c) Convention108 of the Council of Europe.

measures,[13] the recording and disclosure of closed-circuit television (CCTV) footage of a person in the process of committing suicide,[14] the disclosure of a patient's highly-confidential medical information by a hospital, and so forth, have been held to qualify as the processing of data within the meaning of article 2(c) of Convention 108.

The courts have also recognised the fact that certain categories of data merit heightened protection. These are categories of data referred to as sensitive data in Convention 108. These include 'personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life ... [and] personal data relating to criminal convictions'.[15] Consequently, the Court has held that 'fingerprints, DNA profiles and cellular samples, constitute personal data'[16] and that personal information tending to reveal ethnic or racial origin, gender identification, sexual orientation or sexual life, and so forth, belongs to a special category of data subject to heightened protection under article 6 of Convention 108.[17] Other categories of personal information, such as employment records, financial details, meta data of telephone conversations, GPS location data and voice samples, among others, are also the subject of special concern and consideration.[18]

The courts have also held that the data protection dimension of article 8 of the European Convention imposes two types of obligations on state parties, namely, positive and negative obligations. In *Copland v The United Kingdom*[19] the applicant alleged the unlawful monitoring of her telephone calls, emails and internet usages by her employer, a public higher institution/body for which the respondent state is responsible. The Court held that the case 'relates to the negative obligation on the state not to interfere with the private life and correspondence of the applicant' under article 8 of the European Convention.[20] In *Söderman v Sweden*[21] the Court reiterated that article 8 of the European Convention essentially imposes a negative obligation not to arbitrarily interfere with the private and family life of right bearers but that the article also imposes positive obligations on state parties to take measures to secure respect for private life even in relations between individuals *inter se.*[22]

In India there is plethora of statutes and subsidiary legislation regulating the processing of data in the country before 2017, when the Indian Supreme

13 *Uzun v Germany* Application *35623/05* (September 2010).
14 *Peck v UK* [2003] EHRR 287 Application00044647/98.
15 Art 6 Convention 108 of the Council of Europe.
16 *S and Marper v The United Kingdom* Applications 30562/04 and 30566/04 (December 2008) para 68.
17 *Marper* (n 16) paras 66-67.
18 See, eg, *GSB v Switzerland* Application 28601/11 (December 2015).
19 Application 62617/00 (April 2007).
20 *Copland* (n 19) para 39.
21 Application 5786/08.
22 *Söderman* (n 21) para 78.

Court extended the frontiers of the right to privacy in its very popular decision in *Justice KS Puttaswamy (retd) v Union of India*.[23] In *Puttaswamy* the Supreme Court of India found the existing data protection regime inadequate in effectively protecting the privacy and personal data of Indians. The Court held that although not expressly provided for under the Constitution of India, privacy is implied and can be derived from the right to life and personal liberty in article 21 of the Constitution of India. The Court held that privacy was a natural and fundamental human right inherent in all human beings and constituted the important core of any individual's existence because it is a necessary condition for dignified enjoyment of other fundamental human rights.[24]

Furthermore, the Court noted that privacy has at least three dimensions, namely, the protection of individuals' physical body from intrusion; informational privacy; and privacy of choice. According to the Court, informational privacy is an important aspect of the right to privacy. The Court reasoned as follows:

> The old adage that 'knowledge is power' has stark implications for the position of individual where data is ubiquitous, an all-encompassing presence. Every transaction of an individual user leaves electronic tracks without her knowledge. Individually these information silos may seem inconsequential. In aggregation, information provides a picture of the beings. The challenges which big data poses to privacy emanate from both state and non-state entities.[25]

The Court, therefore, underlined the need to regulate the extent to which personal information can be stored and processed by state and non-state actors alike if the balance of power between individuals and state and non-state actors alike is to be maintained.[26] The Court was of the view that '[t]he concept of "invasion of privacy" is not the early conventional thought process of "poking one's nose in another person's affairs". It is not so simplistic. In today's world, privacy is a limit on the government's power as well as the power of private sector entities.'[27]

The Court held that privacy was not an absolute right but can be restricted by a just, fair and reasonable law that passes the test of proportionality and serve a legitimate governmental aim.[28] On this basis, the Court validated the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act 2016 (Aadhaar Act) and its many regulations. The Act and its regulations compel the registration and collection of biometric and other data of citizens for the purpose of issuing them with unique identification numbers as a basis for delivery of benefits and entitlements under the Aadhaar Act. The Court held that although the Act and subsidiary legislation contained wide-ranging provisions invasive of privacy, they are, however, constitutional as they serve a legitimate governmental

23 Writ Petition 494/ 2012.
24 *Puttaswamy* (n 23) 125-126.
25 *Puttaswamy* (n 23) 150.
26 *Puttaswamy* (n 23) 155.
27 As above.
28 *Puttaswamy* (n 23) 158.

purpose of providing subsidies, benefits and services to needy members of the Indian society. The Personal Data Protection Bill 2019, to implement the far-reaching decision of the Supreme Court of India on privacy and data protection in *Puttaswamy*, was initially pending before the Indian Parliament.[29] The Bill, however, was withdrawn on 3 August 2022 in order to incorporate a long list of recommendations of the Joint Parliamentary Committee of the Indian Parliament.[30] At the time of writing, the Digital Personal Data Protection Bill 2023 was being tabled.

In Kenya, the data protection regime evolved from the constitutional right to privacy protected under the Kenyan Constitution.[31] The constitutional right to privacy, therefore, forms the foundation for the data protection regime in Kenya. As such, even before the enactment of a comprehensive data protection regime, the courts adopted expansive interpretations of the right to privacy to protect the personal information of citizens.[32]

Article 31 of the Kenyan Constitution of 2010 guarantees the right to privacy, which includes the right not to have '(a) their person, home or property searched; (b) their possessions seized; (c) information relating to their family or private affairs unnecessarily required or revealed; or (d) the privacy of their communications infringed'.

While the need for a more specific data protection regime led to the enactment of the 2019 Data Protection Act, Kenyan courts have before the coming into force of the Act, protected personal information by relying predominantly on the constitutional right to privacy in the Kenyan Constitution. In *Nubian Rights Forum & Others v The Hon Attorney-General & Others*[33] the High Court of Kenya relied chiefly on the constitutional right to privacy and ruled that the collection of GPS and DNA data pursuant to certain legislative amendments was not a justifiable infringement of the right to privacy of Kenyan citizens. The Court also noted that the data protection regime in Kenya, at the time, was not adequate to cater for concerns related to the protection of the personal information of citizens in relation to the collection of biometric data. To reach this decision, the Court sought to balance the benefits from the collection of citizens' data

29 Chambers and Partners 'India's Personal Data Protection Bill, 2019 – An update' 25 January 2022, https://chambers.com/articles/india-s-personal-data-protection-bill-2019-an-update (accessed 9 July 2022).

30 DLA Piper 'India: Government withdraws long-awaited Personal Data Protection Bill' 4 August 2022, https://blogs.dlapiper.com/privacymatters/india-government-withdraws-long-awaited-personal-data-protection-bill/?utm_source=mailpoet&utmmedium=email&utm_campaign=privacy-matters-newsletter (accessed 4 August 2022).

31 For a comprehensive analysis of how the data protection regime evolved before the enactment of the Data Protection Act by the Kenyan legislature, see AB Makulilo & P Boshe 'Data protection in Kenya' in A Makulilo (ed) *African data privacy laws. Law, Governance and Technology Series* (2016) 317-335.

32 B Andere 'Data protection in Kenya: How is this right protected?' https://www.accessnow.org/wp-content/uploads/2021/10/Data-Protection-in-Kenya.pdf (accessed 30 March 2023).

33 Consolidated Petitions 56, 58 & 59 of 2019 (High Court of Kenya, Constitutional and Judicial Review Division).

against the dangers posed by the collection of the data. By acknowledging the inadequacy of the data-protection regime in Kenya, the Court noted that for the data collection and aggregation process to be justifiable, it ought to be done against the backdrop of a comprehensive data-protection regime. It is worth reiterating that the protection of the rights of the applicants was only possible because of the constitutional right to privacy regime. This is despite the fact that the Data Protection Act became law while the case was pending before the Court.

Furthermore, in *Communications Authority of Kenya v Omtatah Okoiti & 8 Others*[34] the respondents were successful in a privacy infringement lawsuit at the High Court of Kenya where the Court ruled that the device management system (DMS), which sought to collect data from subscribers, was an infringement on the privacy right of the subscribers. Again, this judgment was reached by the Court prior to the enactment of the Data Protection Act. Although the High Court decision was upturned on appeal by the Kenyan Court of Appeal on the ground that the infringing acts alleged had not yet occurred or been implemented,[35] the Court nevertheless ordered the agency to continue with consultation with stakeholders. The Court reached this conclusion by relying solely on the constitutional right to privacy. The primary issue considered by the Court of Appeal was whether the DMS installation was a violation of the right to privacy of the citizens/customers. The Court acknowledged that the DMS was designed to address and protect the interests of the telecommunications operators from the pervasive nature of counterfeit products in the industry. The Court also recognised the fact that the appellant had the statutory power to regulate and license operators and operations in the industry. In the opinion of the Court, seeing that there was no concrete evidence that the agency had concrete plans to violate the right to privacy of citizens other than unsubstantiated statements in the media, the right to privacy could not be said to have been violated. The Court, therefore, noted that the desire for access by the agency was valid and necessary in order to tackle the challenges in the industry and that the agency was acting as a regulator pursuant to its statutory powers. The right, therefore, would be said to have been violated only where the access to the data of consumers was unjustifiable and done without any safeguards whatsoever. Consequently, the Court disagreed with the High Court that mere access to users' data was a violation. This case, therefore, is authority for the view that access to consumers' or customers' data is not in itself a violation as long as it is necessary and justifiable and necessary safeguards for the management of the data are put in place. The Court thus emphasised that access to the data of customers and citizens may be necessary to address certain challenges as long as the access was managed within the purview of certain safeguards. The Court criticised the High Court for being

34 Civil Appeal 166 of 2018.

35 The Court also ruled that the suit was premature since consultations were still being carried out and the agency had not yet implemented the infringing act. This was because the respondents instituted the suit at the High Court on the basis of the appellant's proposals that had not yet been implemented.

overly focused on mere access as the basis for privacy rights violation without attempting to balance the interests of privacy and the mandate of the regulator to tackle the challenges in the industry.

Finally, in *Coalition for Reform and Democracy (CORD) & 2 Others v Republic of Kenya & 10 Others*[36] the High Court of Kenya considered a plethora of constitutional and human rights issues in relation to Kenya's hasty enactment of the Security Laws (Amendment) Act 19 of 2014. In relation to the data privacy issues considered in this case, the applicants had argued that (a) the hastiness in enacting the amendments to the statute was unconstitutional and was in violation of the legislative standing orders, thereby making the process lacking in legitimacy; and (b) the introduction of measures to intercept communication for the purpose of combating terrorism in the amendment was unjustifiable and amounted to a violation of the privacy rights of the citizens. The respondents opposed these arguments and argued that the process of making the statute was necessary and not in violation of the Constitution and the legislative standing orders. Additionally, the respondents argued that the restriction on the citizens' right to privacy was necessary and justifiable in a democratic society. They also argued that the restrictions were necessary for democracy since the objective of the enactment was to prevent terrorist activities. Also, the interested parties aligning with the respondents also argued that the right to privacy was not absolute.

In reaching its decision, the Court noted that since there was reasonable public participation in the process of enacting the law, despite the hastiness in the enactment of the law, the process was constitutional and justifiable in the circumstances. Additionally, in relation to the issue of the validity of the restrictions imposed on the privacy of the citizens, the Court held that the violation was justifiable, constitutional, and did not infringe on the right to privacy. The Court's basis for holding that the restriction was justifiable was that the restriction has a reasonable basis, given the objective of preventing terrorism in Kenya.

A number of conclusions are deducible from the analysis of comparative foreign laws and jurisprudence above. The first is that privacy as a fundamental human right features very strongly in the jurisprudence of the different courts. Second is the fact that data protection is regarded not only as part and parcel of privacy alone, but that it has evolved into a stand-alone right. Third is the fact that even in jurisdictions with expansive data protections frameworks, the intervention of the courts is often needed to fill gaps in the laws and keep the law apace with developments in technology. Detailed features and insights deducible

36 Petition 628 of 2014 consolidated with Petition 630 of 2014 and Petition 12 of 2015 (High Court of Kenya at Nairobi Constitutional and Human Rights Division).

from analysis of comparative foreign jurisprudence done in this part are discussed in part 4 below.

3 Trends and implications of Nigerian courts' jurisprudence on privacy and data protection

Nigeria privacy and data protection framework rests on three principal norms: the Nigerian Constitution via section 37; the Nigerian Data Protection Regulation 2019 (NDPR) promulgated by the National Information Technology Development Agency (NITDA) in 2019; and the newly-enacted Nigeria Data Protection Act 2023 (new Act) which was signed into law in June 2023. Section 37 of the Constitution provides that '[t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'. NDPR on its part provides for the principles of data processing, the lawful basis for processing data, rights of data subjects in Nigeria, among others. The newly-enacted Act, as the substantive and main data-protection framework in Nigeria, preserves NDPR that has been in use since 2019 to the extent that its provisions do not conflict with the provisions of the new Act. This part of the article examines the trends and implications of Nigerian courts' jurisprudence on privacy and data protection in order to decipher judicial approaches and attitudes as well as identify gaps and implications of the existing jurisprudence. The next part identifies learning points for Nigerian courts from comparative foreign jurisprudence analysed in part 2 above.

Ezugwu Emmanuel Anene v Airtel Nigeria Ltd[37] is one of the earliest Nigerian cases on privacy and data protection. In this case the applicant, a lawyer; sued Airtel, his service provider, at the FCT High Court, Abuja on the ground of countless unsolicited calls and text messages by the respondent and third parties to whom the respondent had disseminated his phone number. He claimed that the interference with his solitude violated his constitutional right to privacy. The respondent did not defend the suit. The Court relied on the applicant's evidence to find the respondent liable. An amount of N5 000 000,00 in damages was awarded by the Court against the respondent.

A similar decision was reached in *Godfrey Nya Eneye v MTN Nigeria Communication Ltd*,[38] where the Nigerian Court of Appeal held that disclosure and dissemination by the appellant of the applicant/respondent's mobile phone number without his consent and the consequent unsolicited messages were a violation of the applicant/respondent's right to privacy.

37 Suit FCT/HC/CV/545/2015 (unreported).
38 Appeal CA/A/689/2013 (unreported).

Also, in *Emerging Market Telecommunication Services v Barr Godfrey Nya Eneye*[39] the claimant, a legal practitioner, had sued the operators of Etisalat mobile line for unauthorised exposure or dissemination of his phone number to persons/companies that sent him unsolicited text messages and advertisements. He claimed that this violated his right to privacy under section 37 of the Nigerian Constitution. The Federal High Court found in his favour at first instance. On appeal by Etisalat, the Court of Appeal upheld the decision of the trial court and held that misuse of personal information of the applicant was a violation of the right to privacy under section 37 of the Nigerian Constitution. Damages in the amount of N1 000 000,00 only were awarded by the Court of Appeal against the respondent.

However, in *Adeyemi Ibironke v MTN Nigeria Communications Limited*[40] the appellant alleged that the respondent had surreptitiously obtained and retained information from her SIM card on the respondent's database, and that the respondent send messages to the appellant's phone every 10 to 20 seconds. The appellant contended this action violated her right to privacy and amounted to nuisance, which unduly interferes with her peaceful use and enjoyment of the MTN line. The Court of Appeal observed the following: '[W]as there any credible evidence to, again on the balance of probabilities, establish any breach of privacy by the messages and notification sent to the appellant's sim card, *even if unsolicited*?'[41] The Court answered the question in the negative and held that there was no credible and satisfactory evidence to substantiate the breach of appellant's privacy by the alleged messages or notifications. The Court appeared more disposed to found that the unsolicited and annoying messages amounted to nuisance but not a breach of privacy. Even then, the Court was of the view that credible evidence had not been adduced to ground the claim of nuisance. According to the Court:

> The messages may be inconvenient and sometimes irritating or even annoying since they were unsolicited for and may, in appropriate cases, constitute a nuisance that may be actionable, but the appellant did not set out the details of the messages and notifications which reasonably interfered with his use and enjoyment of the sim card for which he subscribed and was registered with the respondent.[42]

The Court thus implied that unsolicited messages and incessant messages and notifications sent to appellant's phone that disturbed his peace and solitude did not amount to a violation of his privacy. This posture of the Court clearly misapprehended the nature and scope of the changing paradigm of privacy in contemporary times. Such posture, of course, will not effectively protect privacy in the digital age.

39 (2018) LPELR-46193.
40 (2019) LPELR-47483.
41 *Ibironke* (n 40) 32.
42 *Ibironke* (n 40) 32-33.

Also, in *Incorporated Trustees of Digital Rights Lawyers Initiative v LT Solutions & Multimedia Limited*[43] the respondent had offered 200 million Nigerian and international email lists containing other personal information such as age, local government area, state, city and industry of the owners for sale. The applicant sued the respondent on the grounds that the data was published without the consent of the owners; that the respondent had no right or legal basis for the processing of the data; and that the processing violated the rights of the applicant to privacy under section 37 of the Nigerian Constitution. The applicant also alleged that the respondent had breached the provisions of NDPR by failing to publish its privacy policy, which would contain a description of personal information collected, the purpose for the collection of data, the methods of data collection, and so forth, on its website. The High Court of Ogun State per Ogunfowora J held that the right to privacy extended to the protection of a citizen's personal information. The Court, however, held that there was nothing in the affidavit of the applicant to show that consent of the owners of the emails had not been obtained. The Court also held that although it was established that the respondent did not publish its privacy policy as required by NDPR, the Court did not see how this violated the right of the applicant to privacy. Furthermore, the Court held that absent a grant of power in NDPR for state courts and entities to enforce its provisions, a state court is without jurisdiction to adjudicate violations of NDPR. What is clear from this decision is that, despite the fact that the Court acknowledged that the protection of personal information is within the ambit of privacy, the Court in the end did not adopt a rights-based approach to the resolution of the dispute. Otherwise, the Court would not have declined jurisdiction or proceeded on the basis that findings under NDPR are dispositive of the matter. Under the Nigerian human rights regime both state and federal courts can adjudicate violations of human rights, privacy inclusive. A clear implication of the decision will be to restrict the scope of privacy and ability of claimants to litigate their violations in Nigeria.

In *Incorporated Trustees of Digital Rights Lawyer Initiative & Others v National Identity Management Commission*[44] the claimant/appellant's date of birth was wrongly recorded. He approached the respondent to have the information rectified. He was asked to pay N15 000,00 only as administrative charges. The claimant sued the respondent on the ground that he has a right to have the data rectified without cost to him under the section 37 right to privacy provisions of the Nigerian Constitution and clause 3.1(7)(h) of NDPR. At first instance, the trial High Court of Ogun State, per AA Akinyemi J, interpreted the right to privacy rather restrictively. The trial Court held that the right to privacy relates to the protection of the personal spaces and personal information from intrusion. The Court thus linked the right to privacy under the Constitution to the protection of personal information under NDPR. Notwithstanding the linkage,

43 Suit HCT/262/2020 delivered 9 November 2020.

44 *Incorporated Trustees of Digital Rights Lawyer Initiative & Others v National Identity Management Commission* Suit AB/83/2020 (unreported) judgment delivered 15 July 2020.

however, the trial Court held that right to rectification of data under NDPR was not cognisable under the privacy provisions of section 37 of the Nigerian Constitution. The Court, therefore, concluded that no intrusion of personal information had been shown by the claimant. The case was consequently struck out. The claimant, dissatisfied with the decision of the trial Court, appealed to the Court of Appeal. On appeal, the Court of Appeal found that personal information protection comes within the scope of section 37 of the Constitution. The Court was also of the view that NDPR was made in furtherance of the privacy provisions of the Constitution and, consequently, a part thereof. In the final analysis, however, the Court agreed with the trial Court that the right to have data rectified under NDPR was not cognisable under section 37 privacy provisions of the Constitution. The appeal was therefore dismissed for lacking merit.[45]

The clear implication of this decision is that the data subject's rights provided for in NDPR are not cognisable under section 37 of the Constitution and cannot be enforced via the FREP Rules. In other words, they do not amount to fundamental human rights. As has been rightly observed, the Court of Appeal in the case gives with one hand and takes away with another.[46] The non-recognition of the data subject's right to rectification in the case is likely to adversely affect the litigation of other data subject rights under NDPR going forward.

Also, in *Incorporated Trustees of Laws and Rights Awareness Initiative v The National Identity Management Commission*[47] the applicant sued for an injunction to restrain the respondent from further collection and processing of personal data of Nigerian citizens in furtherance of the establishment of a national identity database and issuance of national identity cards to citizens pending the conduct of a data processing impact assessment and independent experts' report on the safety and security of the respondent's operations. The rationale for the injunction was based on reported data breaches in the application rolled out by the respondent for citizens to download their digital identity cards from the Google store. It was claimed that the porous security features and consequent data breaches of the application violated the applicant's privacy under section 37 of the Constitution and Regulation 1.1(a) of NDPR 2019. The Federal High Court, per Ibrahim Watila J, held that that the breach of the data subject's rights under NDPR was not necessarily a breach of the section 37 right to privacy provisions of the Nigerian Constitution, on the ground that Reg 4.2(6) provides that a breach of any provisions of NDPR is to be construed as a breach of the provisions of the NITDA Act of 2007. Thus, the latter provisions take the proceedings outside the ambit of section 37 of the Nigerian Constitution and the FREP Rules. The implication of this decision, of course, is to shut out from the ambit of constitutional and human rights adjudication all issues relating to data

45 (2021) LPELR-55623 (CA).
46 S Okedara and others (eds) *Digital rights in Nigeria: Through the cases* (2022) 50.
47 Suit FHC/AB/CS/79/2020 (unreported).

protection in Nigeria and turn these into mere legal rights under the NITDA Act. This will run contrary to the conception of personal information as part and parcel of privacy under section 37 of the Constitution, as was held in cases such as *Incorporated Trustees of Digital Rights Lawyer Initiative & Others v National Identity Management Commission* by the Court of Appeal above.

In *Digital Rights Lawyers Initiative and Unity Bank*[48] personal data of 53 000 job seekers were exposed on respondent's website. The applicant, on behalf of the job seekers, brought a suit against the respondent and sought a declaration that the respondent's unauthorised exposure of personal data of the job seekers on the internet constituted a personal data breach under Regulation 1.3(xx11) of NDPR; also, that the unauthorised exposure of the personal data on the internet violated the right to privacy of the job seekers as guaranteed under section 37 of the Nigerian Constitution, among others. The Federal High Court, per Ibrahim Watila J, held that the exposure of personal data of persons was not within the privacy provisions of section 37 of the Constitution but only cognisable under the provisions of NDPR. The Court held further that even assuming that section 37 of the Constitution applies, a breach of personal data will qualify as an ancillary claim only and, thus, cannot be enforced via the more expeditious procedure of the FREP Rules, which requires that claims brought under it to be principal human rights claims. The Court also held the action incompetent because the condition precedent to the initiation of the action under NDPR, namely, referral to the Administrative Redress Panel (ARP), had not been complied with, among other grounds relied upon by the Court.

To start with the last ground for the decision of the Court: The opening paragraph of Regulation 4.2 (1) relied upon by the Court as mandating referrals to the ARP in cases of breaches of data subjects' rights in NDPR started with '[w]ithout prejudice to the right of a data subject to seek redress in a court of competent jurisdiction.' A literal reading of this provision clearly preserved the right of data subjects to approach the court with or without referral to the ARP. As has been correctly argued, Regulation 4.2 only empowers the NITDA to set up the ARP.[49] The provision is not intended to fetter the rights of data subjects to approach the courts. The argument that the illegal and unauthorised exposure of personal data does not come within the ambit of privacy or that assuming it does, that it is an ancillary claim also totally misconceived the ambit of the right to privacy and its nexus with data protection. The decision is clearly symptomatic of the traditional and narrow understanding of the right to privacy that has become outdated and obsolete in the current digital age and the onslaught of emerging technologies impacting on the right. The implication of the decision will be to stall the due development of the law and jurisprudence on privacy and data protection in Nigeria.

48 Suit FHC/AB/CS/85/2020 (unreported).
49 Okedara and others (n 46) 85.

Finally, in *Daniel John Daniel v True Software Scandinavia AB (Truecaller)*[50] the applicant sued the respondent for the publication of his phone number to users of the respondent's software without his consent. He contended that the unauthorised publication and disclosure of his telephone number violated section 37 of the Nigerian Constitution, among others. The High Court of Lagos State, per Bola Okikiolu-Ighile J, held that the publication was not a violation of his right to privacy under section 37 of the Constitution. According to the Court:

> A careful review of this shows that the applicant is not a registered member of the respondent's organisation. However, the publishing of the applicant's phone number on the platform of the respondent's software has not shown to me that his right to privacy has been breached. It goes without saying that these facts relied on by the applicant do not disclose any breach of fundamental human right of the applicant.[51]

The Court also held that processes were not properly served outside jurisdiction and that the Court has no jurisdiction. The case was thus struck out. The Court's pronouncement quoted above clearly showed the Court's narrow understanding of privacy in the digital age.

An analysis of the jurisprudence of Nigerian courts above shows that while a few of the cases apprehended the nexus between privacy and data protection and interpreted privacy liberally to cover data protection, a preponderance of the cases conceived the right to privacy in the more traditional sense and disavowed any connection between the two concepts. As rightly observed by Babalola, the case law is 'replete with straightjacketed privacy cases which relate to invasion of homes and offices as opposed to invasion of data privacy *stricto sensu*'.[52] Even in cases that affirmed the connection between privacy and data protection, there was an apparent lack of sufficient and adequate knowledge and appreciation of the technology-driven paradigm of privacy in the current digital age. Another conclusion reached through the analysis of the case law is that the law on the nexus between privacy and data protection remains unsettled with the consequent conflicting decisions of the courts both at the High Court and the Court of Appeal levels. The resolution of this conflict awaits the Supreme Court of Nigeria's intervention.

Granted, most of the cases analysed above were decided under NDPR before the advent of new Nigeria Data Protection Act 2023. The advent of the new Act, however, may not make much difference despite some of its privacy-enhancing provisions, if the courts refuse to interpret the new Act progressively and proactively. First and foremost, no data protection framework, no matter how expansive, will be able to keep pace with current technological developments

50 Suit LH/5868MFHR/2017 (unreported).
51 *Daniel* (n 50) 8.
52 O Babalola 'Nigeria: Data protection and privacy challenges in Nigeria (Legal Issues)' 9 March 2020, https://www.mondaq.com/nigeria/data-protection/901494/data-protection-and-privacy-challenges-in-nigeria-legal-issues- (accessed 11 May 2022).

in the absence of the expansive application of the right to privacy to serve as effective guardrails against inevitable depredations of fundamental human rights, autonomy and freedoms of persons by emerging technologies. Therefore, there is a need for the courts to adopt a proactive and expansive interpretation of fundamental rights and privacy upon which the new Act is hinged. Second, the Act is not likely to be able to cure the narrow and traditional reading of the right to privacy, which is out of tune with contemporary realities of the digital age, in the absence of changed attitudes and perspectives by the courts. Third, the new Act cannot also prevent the decoupling of privacy from data protection in the way it has been done by the courts except if the courts are ready to adopt a more expansive and robust reading of the right to privacy consistent with the tenor and intendment of the new Act and in accordance with comparative foreign jurisprudence and best practices in similarly-situated jurisdictions across the world. The above reasons and many more underscore the importance and necessity of the study even with the coming on board of the new Act.

Thus, drawing insights from comparative foreign jurisprudence discussed in part 2 above, the part below identifies pertinent features of international best practices for Nigerian courts to draw from and resolve their conflicting decisions on privacy and data protection in a bid to usher in a more robust privacy and data protection jurisprudence for more effective protection of the autonomy, well-being and freedom of Nigerians from the harmful effects and depredations of emerging technologies.

4 Insights from foreign law and jurisprudence

The first insight deducible from the analysis in part 2 above is that privacy has two strands: individual interest in avoiding disclosure of personal matters and the independence of individuals in making certain important life decisions. The protection of personal information dimension constitutes the privacy second strand and has birthed the right to informational privacy, that is, data protection, in the United States of America and the right to informational self-determination in Germany. Within the EU, the European Court of Human Rights has also clearly held in cases such as *Z v Finland, PG and JH v The United Kingdom* and *Benedik v Slovenia* that the protection of personal information is fundamental to the enjoyment of the right to privacy guaranteed under article 8 of the European Convention.

The second deducible insight is that data protection flowing from the right to privacy has evolved into a stand-alone right in comparative foreign law and jurisprudence and, thus, is conceptualised as a fundamental human right under both conventional and decisional laws in jurisdictions regarded as best practices. This clearly is the case under the Charter of Fundamental Rights of the EU which guaranteed a stand-alone right to data protection. Decisional laws in India via the Supreme Court of India decision in *Justice KS Puttaswamy (retd) v Union*

of India[53] have also gone a step further to assign the status of a natural right to privacy/data protection upon which the due exercise and enjoyment of other fundamental rights rests.

Third, as discussed in part 2 above, comparative foreign jurisprudence has clearly defined activities or actions that will amount to processing of data flowing from the right to privacy prism. The European Court of Human Rights in *Uzun v Germany* and *Peck v UK* recognised that operations performed on personal information that will qualify as data processing include collection, storage, carrying out of logical and/or arithmetical operations on data, alteration, erasure, retrieval, publication or disclosure, and so forth. Several activities enumerated in the cases as data processing suggest that, with a few exceptions, any handling of personal information whatever will qualify as data processing.

Four, in accordance with international best practices as codified in conventional data protection norms, the European courts of human rights have recognised the special and sensitive status of some categories of personal information referred to as sensitive personal information. These are personal information that tends to reveal racial origin, political opinions and religious or other beliefs and personal information relating to sexual orientation, health status, criminal convictions, and so forth. The Court has thus held in *S and Marper v The United Kingdom,*[54] among others, that this category of personal information is entitled to heightened protection and special concerns and consideration because of their tendency to expose data subjects to harmful differentiation and consequences.

Five, flowing from the right to privacy paradigm, the retention of data beyond the time and objectives for which the data is required is a negation of the control that data subjects should have over their personal information.

Lastly, comparative foreign jurisprudence has also recognised that data protection imposes two levels of obligations on states. In *Copland v The United Kingdom and Söderman v Sweden*[55] the European Court of Human Rights held that privacy and the concomitant right to data protection impose not only a negative obligation on states not to arbitrarily interfere with private and family life, correspondence and personal information of individuals, but also a positive obligation to take measures to secure respect and provide necessary facilities and enabling environment for the protection and full enjoyment of the rights from depredations and violations by third parties. The foregoing are some of the key features and learning points from comparative foreign jurisprudence and laws.

53 As above.
54 As above.
55 As above.

If the courts in cases such as *Adeyemi Ibironke v MTN Nigeria Communications Limited*[56] had recognised the nexus between privacy and data protection and the fundamental nature of privacy-dependent data protection norms in the data-driven era, the Court is not likely to have held that the disclosure of the appellant's phone number to third parties by the respondent and incessant unsolicited messages to the appellant's phone number is not a breach of privacy.

Also, had the courts in *Incorporated Trustees of Digital Rights Lawyer Initiative & Others v National Identity Management Commission* and *Incorporated Trustees of Laws and Rights Awareness Initiative v The National Identity Management Commission* conceptualised data protection as a fundamental right flowing directly from privacy, the courts in those cases would not have held that a breach of data subject rights is not necessarily violation of the right to privacy or that an action for the breach of the right cannot be brought under the FREP Rules.

In addition, if the courts had properly distilled what amounts to data processing in the light of best practices, the Court in *Digital Rights Lawyers Initiative v Unity Bank* would not have held that the disclosure of personal information of 53 000 job seekers on the website of the respondent is not within the ambit of the privacy provisions of section 37 of the Constitution or that the action brought upon it is not cognisable under the FREP Rules. Finally, if the courts had understood the proper scope and ambit of privacy in the digital age in line with international best practices, the Court in *Daniel John Daniel v True Software Scandinavia AB (Truecaller)* would not have held that the publication and disclosure of the applicant's details by the respondent to users of the respondent's software was not a violation of applicant's constitutional right to privacy.

An analysis under this part reveals that Nigerian courts have a lot borrow from comparative foreign jurisprudence for a more robust and effective privacy and data protection regime in Nigeria.

Fortunately, the new Act contains provisions that strengthen the constitutional, privacy and fundamental rights approach to data protection in Nigeria. First, unlike NDPR that approached data protection from a statutory rights point of view, the new Act directly connects the protection of personal information of data subjects to the protection of fundamental rights guaranteed under the Constitution of Nigeria.[57] Second, the new Act, while exempting the processing of personal data done solely for personal or domestic purposes, subjects the exemption to the fundamental rights to privacy of data subjects.[58] Third, the new Act also confers a right on a data subject to object to the processing of personal data.[59] Where a data subject objects to the processing of his or her personal data,

56 As above.
57 Sec 1(1)(a) Nigeria Data Protection Act 2023.
58 Sec 3(1) Nigeria Data Protection Act 2023.
59 Sec 36(1) Nigeria Data Protection Act 2023.

a data controller is obliged to cease further processing of the data unless the data controller can demonstrate public interests or legitimate grounds that override the fundamental rights, freedoms and interests of the data subject.[60] Four, there is a right of data subjects to object to processing of their personal data for direct marketing purposes.[61] Where a data subject objects to such processing, the data shall no longer be processed by the data controller.[62] Five, data subjects also have a right to object to the processing of personal data that is based mainly on the automatic processing of personal data.[63] The objection will not apply where the processing is required for the performance of a contract between a data subject and a data controller or where the processing is authorised by a written law that provides for necessary measures to protect the fundamental rights, freedoms and interests of data subjects.[64] Finally, in all circumstances of automatic processing of personal data, the data controller is mandated to implement measures to protect the fundamental rights, freedoms and interests of data subjects.[65]

The foregoing provisions clearly demonstrate that the new Act approached data protection from a constitutional, privacy and fundamental human rights perspective. This is an approach upon which counsel and litigants can leverage to persuade courts to depart from decisions that appear not to lean in favour of fundamental rights and privacy. In addition, rooting data protection in privacy and fundamental rights and freedoms in the Constitution, as was done in the Act, suggests that the various data subject rights under the new Act will be amenable to enforcement through the FREP Rules.

5 Conclusion

This article interrogates the trends, approaches and implications of Nigerian courts' jurisprudence on privacy and data protection. The need for and importance of the interrogation are set out in the introduction. Part 2 examines the changing conceptualisation and paradigms of privacy underpinned by changing technology and data-driven approaches in comparative foreign jurisprudence. It was found that the notion of privacy now is much more than a mere right to be let alone and is now a more complex and eclectic concept to engage with the drastically-changing society and technology. Part 3 analyses Nigerian case law on privacy and data protection. It was found that while a few cases interpreted privacy liberally and affirmed the connection between privacy and data protection, a preponderance of the cases follow the straight-jacketed and traditional conception of privacy and disavowed any connection between privacy and data protection. Even cases that appear to be more progressive show an apparent lack

60 Sec 36(2) Nigeria Data Protection Act 2023.
61 Sec 36(3) Nigeria Data Protection Act 2023.
62 Sec 36(4) Nigeria Data Protection Act 2023.
63 Sec 37(1) Nigeria Data Protection Act 2023.
64 Sec 37(2) Nigeria Data Protection Act 2023.
65 Sec 37(3) Nigeria Data Protection Act 2023.

of understanding and awareness of what privacy entails in the digital age. The foregoing scenario gave rise to conflicting decisions of the courts at both the High Court and Court of Appeal levels. Part 4 identifies pertinent features of comparative foreign jurisprudence that can serve as learning points for Nigerian courts. Provisions of the new Act that strengthen privacy and fundamental rights and upon which counsel and litigants can leverage to persuade courts to lean in favour of fundamental rights and privacy in their interpretation of the new Act were also highlighted and discussed.

The courts have a critical role to play in the development of the privacy and data protection norms of any country in the current data-driven era. No regime, no matter how explicit and expansive, will keep pace with the current level of development in technology. The right to privacy is the last bastion of hope to serve as effective guardrails against inevitable depredations of autonomy and freedoms inherent in the continued expansion and developments of emerging technologies. The mantle, therefore, falls on the courts to interpret privacy liberally and expansively to particular and live cases, thereby developing the privacy jurisprudence on an ongoing basis. The courts will be able to do this only if seized of the appropriate conception of privacy and data protection.

Going forward, the liberal and proactive approaches and best practices from comparative foreign jurisprudence discussed in this article are commended to Nigerian courts. This will equip them with the appropriate conceptualisation to discharge the critical burden they bear in this regard. The privacy and fundamental rights-enhancing provisions of the new Act identified in this article are also commended to the courts in their interpretation and enforcement of the provisions of the new Act. Finally, the courts are encouraged to approach data subject rights under the new Act as fundamental human rights amenable to adjudication and enforcement via the FREP Rules consistent with the intendment and tenor of the new Act.

African Journal on Privacy & Data Protection

To cite: D Sato 'Modern problems require modern solutions: Data protection and the right to privacy in national social support programmes in Malawi' (2024) 1

African Journal on Privacy & Data Protection 119-151
https://doi.org/10.29053/ajpdp.v1i1.0007

Modern problems require modern solutions: Data protection and the right to privacy in national social support programmes in Malawi

*Daniel Sato**
Lawyer, Malawi

Abstract:

The right to privacy is a basic right, which is closely associated with the right to dignity. The piloting of information processing technology has heightened the risks associated with information processing, therefore presenting a modern problem. In Malawi, the government through the Department of Economic Planning collects mammoth personal information used in social support programmes through a framework termed the Universal Beneficiary Registry. The information is used by the government and various social support partners. The article notes that this information is disposed to various risks, possibly violating the right to privacy of an individual or a group of individuals. The article investigates the safeguards that are there under the Unified Beneficiary Registry for the protection of the right to privacy. It concludes that the Unified

* BA; LLB (Malawi); satochikondi@gmail.com. At the time of writing and submitting this paper, the only comprehensive law on data protection in Malawi, the Data Protection Bill of 2021, remained in draft form. However, at the time of publishing, the Data Protection Bill had been passed into law having been introduced as Bill No 22 of 2023. The bill has been assented to by the President and is now the Data Protection Act. Once gazetted, it immediately or on the date appointed in the gazette becomes part of the Laws of Malawi.

Beneficiary Registry has taken reasonable steps to safeguard the data that it holds through technical and organisational measures. Regardless, it is opined that lack of a comprehensive legal regime on data protection might impact efforts to protect data under the UBR in Malawi. The article recommends that the area of data protection/privacy law needs urgent reform to address these contemporary problems.

Key words: privacy; data; data protection; Unified Beneficiary Registry; MNSSP II

1 Introduction

The evolution of advanced information and communication technologies has streamlined the collection of extensive amounts of personal data. Personal data is increasingly collected, generated, stored and utilised by institutions both in the public and private sector. Collected data is utilised in the provision of healthcare, health and other types of insurance, education, banking and financial services and hospitality services. Information technologies (Its) have also enabled the assortment of personal data in the delivery of social programmes.

When it comes to National Social Support Services (NSSPs),[1] information and communication technologies are now used to collect and store information about people for development programmes.[2] This serves various purposes such as targeting of beneficiaries in national social support programmes and has various benefits such as the avoidance of duplication of efforts.[3] It allows various players in NSSPs to have critical data that helps in decision making based on areas of need, among some motivations.

The article's focus borders on data collected by the government for National Social Support Programmes (NSSPs) under the Unified Beneficiary Registry (UBR) framework in Malawi.[4]

Until recently, Malawi lacked a legal framework to address data protection and privacy issues. There has been a marked shift with the adoption of laws that

1 The Malawi National Social Support Programme is an initiative aimed at strengthening social support and social protection to persons whose living standards are vulnerable. It currently is in its second phase and the focus under this second phase is partly integration through linkages, concerted monitoring and strengthened systems including data collection and management systems; Malawi National Social Support (MNSSP II), March 2018. Also see https://socialprotection.org/discover/legal_policy_frameworks/malawi-national-social-support-programme-mnssp-ii (accessed 15 September 2023).

2 B Wagner & C Ferro 'Data protection for social protection: Key issues for low- and middle-income countries' Working paper for the GIZ (Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)) GmbH.

3 As above.

4 The UBR is a database used by various social support programmes in Malawi. Its core function is to provide a single source of data and data processing for various social protection programmes. It allows various social protection players to target their beneficiaries. It was introduced in 2016. See https://www.impactpool.org/jobs/737267 (accessed 20 September 2023).

seek to protect personal data of individuals.[5] For organisations that bothered to have data policies, they organised their data policies in ways that fit their thinking of data protection and privacy. Nevertheless, in the past years there has been a surge in legislative attention in this domain.[6] These include the enactment of the Electronic and Cyber Security Act and the drafting of the Data Protection Bill signifying a contribution to data protection as well as a marked growth of interest in this realm.

Among these progresses and the intensifying expansion of data collection and processing, the government introduced the Unified Beneficiary Registry (UBR).

2 Unified Beneficiary Registry

The UBR is a centralised database. Under it, the government in collaboration with various development partners collects data about human targets for various development programmes.[7]

The primary role of the UBR is to support targeting of households with potential interventions that are likely to have a positive outcome on their day-to-day livelihood.[8]

The UBR collects and stores data to enable programme planners and implementers in social protection programmes to target households more efficiently and effectively using information and communication technology services.[9] Furthermore, the UBR offers an interface for access, exploiting and sharing data based on the specific requirements of the discrete social protection programmes.[10]

As additional data continues to be collected under the UBR, the amount of (sensitive) information on the table of risk against manipulation increases and so does the risk for unauthorised access, accidental damage and disclosures among some. Also, with ongoing developments in information and communication technology, problems concerning the right to privacy emerge. This article highlights the need for modern solutions to address these potential risks on violation of the right to privacy.

5 J Kainja 'Privacy and personal data protection: Challenges and trends in Malawi' (CIPESA September 2018), https://cipesa.org/?wpfb_dl=300 (accessed 23 August 2022).
6 As above.
7 https://www.ubr.mnssp.org/?page_id=2 for information on the Universal Beneficiary Registry (accessed 23 August 2021).
8 Kainja (n 5).
9 UBR (n 4).
10 As above.

The initiation of data-driven technologies and data sharing between many entities gives rise to a range of legal complexities.[11] Some of the issues of interest in data and data management include privacy of data subjects and data sharing; breaches of related obligations in a data exchange or access transaction; data sharing obligations; data sharing agreements (DSAs); and liability in cases of breach.

The subject of privacy protection has evolved over the years. In the digital era, privacy laws and regulations have risen to prominence largely because of the simplicity with which data collection, keeping and transmission are done and, therefore, potential risks accmpanying it. Traditionally, the right to privacy is not an easily-defined concept owing to various social factors and expectations of the self, which sometimes blur the lines on where privacy must start and end.

Prior to the seminal article 'The right to privacy' by Warren and Brandeis,[12] there was limited discourse within academic circles regarding the right to privacy and the inevitability for data protection to safeguard the interests of data subjects. The notion of privacy now is possibly well-established. Nonetheless, it becomes more complicated with the dawn of digital technologies.

Before the introduction of information technologies, details of individuals were collected and recorded on paper. Solove notes that details of individuals were easily forgotten and destroyed by the collectors.[13] Still, the advent of information technologies has enhanced opportunities for public and private organisations to process personal data, enabling data retention easily without the limitations of physical storage space. As Clarke notes, this poses various risks,[14] as noted earlier.[15]

Additionally, it would thus be argued that digital technologies have made it easier to transact in data with remarkable risks due to the faith entrusted to a single controller. Once data is collected and stored in a database, more control essentially is given to the controller.

In addition to the risks associated with data collection espoused above, the problem of lack of knowledge of data flows by a data subject and blacklisting also becomes apparent once data is transferred into a database such as the UBR.[16]

11 AB Makulilo (ed) *Law, governance and technology series: African data privacy laws* (2016).
12 SD Warren & LS Brandeis 'The right to privacy' (1890) 4-5 *Harvard Law Review* 193-195; it is a work of note on the history of the right to privacy with vast scholarly recognition.
13 DJ Solove 'Conceptualising privacy' (2002) 90 *CLR* 1088.
14 R Clarke 'Information technology and datavaillance' (1988) 31 *Communications of ACM* 505-508; see also AM Froomkin 'The death of privacy?' (2000) 52 *Stanford Law Review* 1472. The risks intimated include lack of knowledge of potential uses, dangers of stalking and discrimination by governments.
15 Warren & Brandeis (n 12).
16 Clarke (n 14).

Empirically, the case of Bodil Lindqvist v Åklagarkammaren i Jönköping[17] provides a classic example of data protection breaches. In this case, sensitive health data of individuals was exposed on the internet. It can be comprehended, therefore, that the UBR is not intrinsically insusceptible to possible risk of unauthorised access or disclosures of the data it contains. Effects of data breaches can cost information holders a fortune. Mobile communications giant T-Mobile has been on the receiving end of consequences of data breaches wherefrom it was forced to settle a claim centering around 'unauthorised access' to a section of customer data that was put up for sale on a known cybercriminal forum.[18]

With these fears based on technological advances, the legal response has been to enact data protection legislation. Whereas data protection laws have been enacted in other jurisdictions, and are used to regulate data processing, including the imposition of fines, as in the T-Mobile case, other countries such as Malawi are yet to implement robust legal systems to address these fears.

Whereas it will be seen that technology has largely played a part in data protection laws, Bygrave expands on other catalysts for the advent of data protection laws.[19]

Bygrave explores three primary influences driving the development of data protection laws.[20] First, he attributes technological evolution and related trends as a key driver for devising of data protection laws. Under this category, Bygrave highlights that growing volumes of stored data and its cross-border sharing have created a demand for safeguards to protect personal data. The second driver is attributed to increased public fears relating to privacy and multifaceted principles relating to data protection. Lastly, Bygrave notes that the interest developed by international legal instruments has influenced a proliferation of data protection laws in domestic and other international dispensations.

Nevertheless, in 2004 Bygrave expanded his drivers to embrace philosophical aspects, distinguishing them as indispensable in determining the levels of privacy within a given society.[21] Under this conception, privacy is tied to value systems of each individual society. For instance, Bygrave notes that societies with liberal ideas are more likely to exhibit a higher concern for privacy.

17 ECJ Case C-101/01; AB Makulilo 'Does the Lindqvist decision by the ECJ make sense in terms of its treatment of the application of art 25 of Directive 95/46/EC to uploading and downloading of personal information on internet homepages? Tutorial Paper, cm, Norwegian Research Centre for Computers and Law (NRCCL) 2006.

18 https://www.csoonline.com/article/567531/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html (accessed 20 September 2023).

19 LA Bygrave 'Privacy and data protection in an international perspective' (2010) 56 *Scandinavian Studies in Law* 175.

20 As above.

21 As above.

Nevertheless, whatever the philosophical thinking behind data protection might be, it can only be argued that technological advancements are the major catalyst for privacy laws.

Unregulated data processing has the potential to result in human rights violations, including infringements on the rights to privacy, dignity, security of the person, property and to be free from discrimination without lawful excuse.[22] Unregulated data processing has also been feared to pose identity theft,[23] harassment and stalking,[24] as well as targeting risks, among other risks.[25] The T-Mobile case study above clearly illustrates that personal data may be of immense interest to criminals.

This article analyses the extent to which the UBR framework, the largest of any data processing scheme in Malawi (apart from compulsory civil registration), protects personal data of its subjects in its processing and sharing framework, in line with domestic and international data protection law.

The article employs a desk research methodology and adopts the UBR's data management and sharing protocols as a reference point for analysis for data protection laws in Malawi. The underlying assumption is that the UBR falls short from adequately safeguarding the right to privacy of data subject, primarily attributed to the lack of a definite and robust legal framework for personal data protection in Malawi.

3 UBR in context

Prior technical assessment has shown that the UBR is prone to risks such as the lack of a firewall to guard against intrusion.[26] This has the potential of invading data subjects' privacy. Prior legal assessment of the UBR does not exist in the

22 G Sartor 'Human rights in the information society: Utopias, dystopias and human values' in M Viola de Azevedo Cunha and others (eds) *New technologies and human rights: Challenges to regulation* (2013) 14-24; P Ferreira 'Angels and demons: Data protection and security in electronic communications' in M Viola de Azevedo Cunha and others (eds) *New technologies and human rights: Challenges to regulation* (2013) 203-216.

23 See generally E Aimeur & D Schonfeld 'The ultimate invasion of privacy: Identity theft' Ninth Annual International Conference on Privacy, Security and Trust 2011, www.site.uottawa.ca/~nelkadri/CSI5389/Papers/8-Aimeur_and_Schonfeld_PST2011.pdf (accessed 22 August 2021).

24 S Sissing & J Prinsloo 'Contextualising the phenomenon of cyber stalking and protection from harassment in South Africa' (2013) 2 *Acta Criminologica: Southern Africa Journal of Criminology* 15, 19-20.

25 Eg, China is using technology to monitor, control and target people. See X Qiang 'Dataveillance' in Xi Jinping's Brave New China" *Power 3.0* 26 April 2018, www.power3point0.org/2018/04/26/dataveillance-in-xi-jinpings-brave-new-china/ (accessed 22 August 2021); S Feldstein 'The road to digital unfreedom: How artificial intelligence is reshaping repression' (2019) 30 *Journal of Democracy* 40-45.

26 K Lindert and others 'Rapid social registry assessment: Malawi's Unified Beneficiary Registry', https://openknowledge.worldbank.org/handle/10986/31012 31 (accessed 18 October 2021).

public sphere and the UBR being a relatively modern project, not much research has been done surrounding its legal implications.

Additionally, elsewhere prior research on data processing provides thorough views on privacy, data management and the risks of information processing, hence requiring protection.[27] In Malawi, these views are largely wanting owing to the absence of extensive prior research in this area. Yet, a researcher has explored this field through her Master's thesis, focusing on the right to data privacy for individuals in underprivileged societies.[28] Her hypothesis centres on the concept that socio-economic experiences amplify the risks and instances of violations concerning the right to privacy and data protection.[29]

As alluded to, this article employs a legal audit approach on the UBR. Relatively, data privacy is a whole new area in Malawi. As at the time of writing this article, the primary endeavour toward a data protection law was still in draft format, personified in the Data Protection Bill. This position is in contrast to the time of the previous study steered by Nyemba.[30] Additionally, unlike the previous study, this study focuses on a practical setting and seeks to analyse the intersection of the law and practice in the workings of the UBR. With an ambitious project such as the UBR and, potentially, other projects, it is pertinent to study the status of the law providing for data protection in Malawi as it meets practice.

4 A research framework

The perceptions of privacy and data protection are crucial to any study in the domain of the right to privacy in digital technologies.

27 Makulilo (n 11). Makulilo studies the status of data protection in sub-Saharan Africa. He appreciates the need to protect personal data but concludes that the regulatory scheme is still in its infancy in most sub-Saharan countries.

28 C Nyemba 'Right to data privacy in the digital era: A critical assessment of Malawi's data privacy protection regime' GC Publications, 2018/2019, https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1829/Nyemba%20HRDA.pdf?sequence=1&isAllowed=y (accessed 22 August 2021).

29 As above.

30 As above.

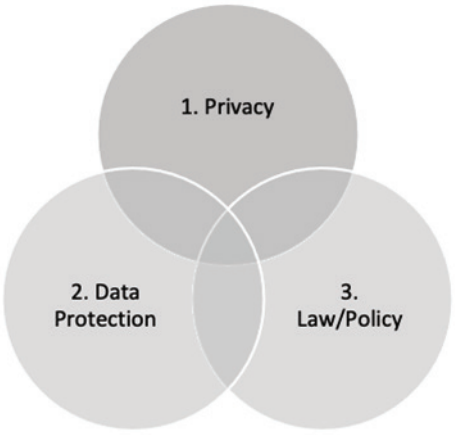

Figure 1: Article's thematic concepts

There arguably are various contested concepts of data protection and privacy.[31] To better understand the challenges surrounding data protection and privacy concepts, the article proceeds to elucidate the main thematic concepts as well as the manner in which they relate to one another. Conceptually, the understanding in this article is that data protection is a resultant concept that is used to guarantee privacy of the subjects to which data relates. Figure 1 presents the thematic concepts of the article and their intersection with the law.

From figure 1, the guiding understanding is that the concept of data protection itself is guided by privacy considerations. The right to privacy; and the concept itself, largely inform the need for data protection. Data protection in its entirety is a legal and policy mechanism that ensures privacy of individuals to which data relates. Nonetheless, a caveat must be stated at the outset that data protection is not entirely about the right to privacy.[32] Data protection may be achieved through legal and policy mechanisms.

4.1 Privacy, a jurisprudential term?

Privacy as a legal concept is a contested term.[33] Outside legal scholarship, the conception of privacy is also largely relative to various social and cultural phenomena. As Young eloquently argued, 'privacy is like an elephant; it is more

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

32 C Kuner 'An international legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law Security Review* 308.

33 Mulligan (n 31).

readily recognised than described'.[34] This implies that the concept of privacy is subjective and can mean different things to different individuals.[35]

As illustration, Mr X may not have a problem sharing his address with the public. Therefore, he would not have problems with settings on social media platforms that display his address. Mr X's wife, on the other hand, considers her address very private information. She would consider such details amenable to decisional privacy. This illustrates the simple but delicate issue of privacy being a relative and contested concept.

What, then, is the essence of the notion of privacy? By tradition, the right to privacy or to one's person was conceived as the right to be free from interference or intrusion, to be left alone.[36] In this setting, the expression 'right to privacy' does not denote a legal requirement for privacy but rather signifies the individually-abstracted need to be left alone. Privacy as the right to be left alone was popularised by the American authors Warren and Brandeis.[37] Unpacking the idea that the person has an entitlement to be let alone essentially is accepting the notion that the person has some immunity from interference, subject to other lawful overriding interests that may be sought over this immunity by the state or authorised private actors. Such lawful interests would be social security, as in the case of the UBR. However, the qualification is that for privacy interference, the same must be lawful. It would be argued that this extends to the processes after the initial privacy disruption.

The traditional conception of privacy is narrow in modern dispensation. It arguably sets off from an understanding that every individual has personal confines that must not be accessed without the person's consent. Perturbed by the arguably waning conception of privacy, Westin was among the first scholars to attempt a reformulation of the concept of privacy.[38] Westin articulated privacy as 'the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others'.[39]

Westin's definition assumes that the determination of privacy question invariably is within the discretion of the individual in question and, thus, leaning towards decisional privacy. However, such a conception would seem to be inconsistent with the term 'privacy' itself and renders the term, as earlier feared, subject to inconsistences of application. The definition of privacy should extend to the claims that the law may also impose. Nonetheless, Neethling appears to

34 C Goodwin 'Privacy: Recognition of a consumer right' (1991) 10 *Journal of Public Policy and Marketing* 149.
35 AR Miller 'The assault on privacy: Computers, data banks, and dossiers' (1971) 22 *Case Western Reserve Law Review* 808; also see Goodwin (n 34).
36 R Allen & A Turkington *Privacy law: Cases and materials* (2002).
37 Warren & Brandeis (n 12) 193.
38 As above.
39 As above.

agree with Westin, stating that the self-determination of interests in information is the fundamental basis of an individual's privacy.[40]

Even so, the overarching tenet in the conception of privacy is that, therefore, there is a will to exclude certain information from publicity. This research adopts the approach that privacy encompasses both decisional, legal and policy interests.

5 Theoretical underpinnings

5.1 Information control theory

One of the most well-known theories of privacy is the information control theory. Westin's classical privacy theory is of particular illumination. The information control theory has two main propositions. The initial assumption is that individuals possess control over their personal information concerning data controllers or data processors. The second assumption, as a substitute to the first, suggests that individuals can potentially impact the information practices of data related to them.

According to Westin's theory, 'privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[41] The sentiments in Margulis's conception of information control echo those of Westin. Margulis states that 'privacy, as a whole or in part represents control over transactions between person(s) and other(s), the ultimate aim of which is to increase autonomy and or to minimise vulnerability'.[42]

The information control theory has several variants. Tavani has attempted to provide a summary of some of these variants:

> According to Fried, privacy 'is not simply an absence of information about us in the minds of others, rather it is the control over information we have about ourselves' (1990, 54). Miller embraces a version of the control theory when he describes privacy as 'the individual's ability to control the circulation of information relating to him' (1971, 25). A version of the control theory is also endorsed by Westin ... and Rachels appeals to a version of the control theory of privacy in his remarks concerning the connection between 'our ability to control who has access to information about us and our ability to create and maintain different sorts of relationships' (1995, 297).[43]

40 J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 18.
41 AF Westin *Privacy and freedom* (1967) 7.
42 ST Margulis 'privacy as a social issue and behavioural concept' (2003) 59 *Journal of Social Issues* 245.
43 HT Tavani 'Philosophical theories of privacy: Implications for an adequate online privacy policy' (2007) 38 *Metaphilosophy* 3, cited and critiqued in Makulilo (n 11).

The information control theory, as observed by Makulilo, faces criticism.[44] The primary objection is that the theory erroneously assumes that privacy inevitably is intrinsically affected when an individual discloses information. I respectfully disagree. A person does not necessarily lose privacy when they no longer have control; their privacy is only made vulnerable. Additionally, the loss of control also essentially reduces their autonomy, as duly noted by Margulis.[45] This critique is further refuted by Davis who maintains that the relinquishment of control does not equate a loss of privacy. Consequently, privacy may be compromised even when control has not been fortified.[46] In effect, the theory advocates greater information control by the subject.

The criticism mentioned above leads to another critique of the information control theory, highlighting its failure to segregate between actual and potential violation of privacy.[47]

Despite the criticisms levelled against the information control theory, it is measured as one of the most directly applicable theories to address issues related to data processing by organisations.[48] The information control theory also aligns with the fundamental principles of data protection law, emphasising increased involvement of data subjects, including their ability to influence the processing of information about themselves.[49] Additionally, the theory imparts significant regulatory influence to the concept of privacy, enabling advocates of data protection law to explore the principled dynamics and self-determination involved data processing.[50]

The information control theory and its propositions will be employed to analyse whether data protection law in Malawi offers and enables information control by data subjects to ensure data protection of data subjects.

5.2 Pragmatism theory

The major proponent of this theory is Solove.[51] He advocates a bottom-up approach in dealing with privacy issues. His approach basically is that privacy issues must be looked at pragmatically. In essence, this postulation is that the law must provide room for analysing privacy considerations in the context in

44 Makulilo (n 11).
45 Margulis (n 42).
46 S Davis 'Is there a right to privacy?' (2009) 90 *Pacific Philosophical Quarterly* 451.
47 D Elgesem 'The Structure of rights in Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data' (1999) *Ethics and Information Technology* 290; R Volkman 'Privacy as life, liberty, property' (2003) 5 *Ethics and Information Technology* 203.
48 LA Bygrave 'The place of privacy in data protection law' (2001) 24 *University of New South Wales Law Journal* 282.
49 As above.
50 As above.
51 DJ Solove 'Introduction: Privacy self-management and the consent dilemma' (2013) 126 *Harvard Law Review* 1879, 1880.

which they occur. Privacy, in his view, is not a concept that can apply universally to different situations. Solove's bottom-up approach calls for an understanding of privacy from scenario-specific circumstances such as a disruption of practices, disturbance of peace of mind, among possible situations.[52] In examining the practices under the UBR, it is important to analyse whether in the context of the law, the UBR's practices offer pragmatic responses to data protection. One of the ways in which to assess this in Solove's lens is whether data subjects can still be said to have control over their personal information.

The pragmatism theory can be said to agree with the conception of data protection as postulated by De Hert and Gutwirth who note that data protection is a necessity on the assumption that that private and public actors need to be able to nonetheless use personal information because it benefits the society. The conception therefore is that data protection is not a means to prevent data processing, but a vehicle to promote justifiable data processing[53].

The pragmatism theory is not without criticism. One of the major criticisms is that it renders itself to so much subjectivity rendering the safeguard of privacy in the balance by promoting vagueness and ambiguity in the conception of privacy[54]. However, it is argued that this subjectivity may be controlled by means of legislative ingenuity that seeks to control data processing practices, while giving room for data processors to make privacy choices in the confines of a particular regulatory environment. For instance, one way of achieving this is requiring data processors to disclose reasons for the actions that they take in regard to the data that they process. Another criticism to the pragmatism theory is that regardless, the legislature would need to have a working concept of privacy to better define the parameters in which it applies. The critics argue that divorcing the understanding of privacy from any theory is to argue in circles.[55]

Regardless of the criticisms, the pragmatic theory provides explanations of legislative practices and the different approaches taken in tackling the question of privacy. In this regard, it is important as it helps to analyse whether the legal environment in data protection in Malawi is flexible to accommodate various privacy questions. Additionally, it will be useful to analyse whether it gives room to data processors to address privacy questions based on the understanding that data processing is inevitable nonetheless, more specifically, and in relation to the study objectives and whether or not Malawi's municipal laws are based on pragmatic considerations.

52 As above.
53 As above.
54 DK Mulligan 'Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy(, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5124066/ (accessed 14 February 2024)
55 A Thierer 'Book review: Solove's *Understanding Privacy*' (2008) *The Technology Liberation Front* https://techliberation.com/2008/11/08/book-review-soloves-understanding-privacy (accessed 14 February 2024)

6 Modern problems require modern solutions: A juxtaposition of data protection in relation to the right to privacy

Data protection laws are increasingly being adopted world over in response to concerns and problems of privacy invasion through data processing. This partially is attributable to the easiness in record keeping, which further accelerates risks associated with access and disclosure of information, among others.[56]

The term 'data protection' is regarded as having originated from the German term *datenschutz*.[57] Under this etymological conception, data protection is understood as the relationship between the collection and dissemination of data, the use of technology or other means and the public expectation of privacy, as well as the legal and political (and policy) issues surrounding them.[58] At its core, data protection in the sphere of pragmatism accepts that data about individuals has to be used but being cautious with the need to safeguard an individual's privacy preferences and personally identifiable information.[59]

Bygrave notes that data protection need not always involve legal measures.[60] Indeed, as noted by Michael and others,[61] there are various parameters to data protection, which include political, social and public expectations of privacy, among others. Bygrave thus describes data protection as deliberate legal and non-legal procedures undertaken to safeguard data subjects from detriment that may result from data processing of data about themselves. He further understands it to include the various philosophies, values and ethics attached to data processing.[62]

As noted by Michael and others,[63] data protection also encompasses societal understanding of the term itself. One of the most noted socio-definitions of data protection is Podlech's 1976 definition that (data protection) is 'promulgating and adopting conditions for data processing in a particular society, to meet acceptable standards in that particular society'.[64]

It is thus argued that data protection encompasses the legal and policy safeguards of a person's privacy (throughout referred to as the data subject) with regard to the processing of data concerning themselves by another person or institution.

56 Bygrave (n 17).
57 MG Michael *Uberveillance and the social implications of microchip implants: Emerging technologies* (2014).
58 As above.
59 V Torra *Introduction, data privacy: Foundations, new developments and the big data challenge* (2017) 1-21.
60 Bygrave (n 48).
61 Makulilo (n 11).
62 UBR (n 4.)
63 Makulilo (n 11).
64 A Podlech. *"Gesellschaftstheoretische Grundlage des Datenschutzes." In Datenschutz und Datensicherung,* edited by R Dierstein, H Fiedler, and A Schulz, 311- 326. Köln: J. P. Bachem Verlag.

The right to privacy is a fundamental human right recognised as such by various international instruments, including the Universal Declaration of Human Rights (Universal Declaration) and the International Covenant on Civil and Political Rights (ICCPR). It has been touted as a fundamental value of legal protection by the Australian Law Commission.[65] Article 17 of ICCPR, to which Malawi is a party, provides:

> (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> (2) Everyone has the right to the protection of the law against such interference or attacks.[66]

In relation to data protection, Kuner argues that privacy is a concept that is independent from data protection although the former should be considered more broadly. Kuner nonetheless acknowledges that there is a significant synergy between the two concepts, with privacy considerations being considered a vital driving force behind data protection practices and requirements.[67]

Despite there being an overlap between the two concepts, the question that normally is asked is whether privacy and data protection are one and the same thing. Cuijpers[68] raises this question and answers in the negative, concurring with Block that privacy and data protection essentially are different.[69] The two argue that since an individual's right to privacy safeguards an undisturbed private life and offers the individual control over intrusion of the private sphere, it is different from protection of the individual with regard to the processing of personal data, which is not restricted to the private sphere of the individual.[70]

Makulilo makes a very insightful observation in his doctoral thesis. He notes that regardless of the fact that scholars continue to argue that although clearly engrained in privacy protection, *data protection* does not necessarily exclusively raise *privacy* issues.[71] De Hert and others argue that the concept of privacy involves prohibitive rules that require 'don'ts', whereas the concept of data protection includes rules that organise and control the way personal data can only be legitimately processed if some conditions pertaining to the transparency of the

65 https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-dp-80/2-guiding-principles/principle-1-privacy-is-a-fundamental-value-worthy-of-legal-protection/ (accessed 22 March 2022).
66 International Covenant on Civil and Political Rights (ICCPR) 999 UNTS 171 art 17.
67 C Kuner 'An international legal framework for data protection: Issues and prospects' (2009) 25 *Computer Law and Security Review* 308.
68 C Cuijpers 'A private law approach to privacy: Mandatory law obliged?' (2007) 4 *SCRIPTed* 312.
69 Makulilo (n 11).
70 As above.
71 Makulilo cites P de Hert & E Schreuders 'The relevance of Convention 108' 33 42 Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19-20 November 2001, cited in 'EU study on the legal analysis of a single market for the information society', November 2009, ch 4, 4.

processing, the participation of the data subject and the accountability of the data controller are met.[72]

De Hert and Gutwirth further distinguish between privacy and data protection based on their respective objectives, although they emphasise that the objectives align with the two concepts.[73] Nonetheless, they think such an equation would be a narrow conception. They argue that the main aim of data protection is to protect data subjects from unjustified data processing. This understanding, according to De Hert and Gutwirth, is on all fours with the right to privacy that seeks to safeguard against unjustified interferences in one's personal life. From this understanding, they argue that this might inform many scholars' attitude to consider data protection and privacy interchangeably.

De Hert[74] and Bygrave[75] appear to share a fundamental agreement, namely, that privacy undeniably holds a central role in data protection law, but labelling data protection law as solely or even primarily focused on safeguarding privacy is misleading.

Truly, in the case of *Bavarian Lager Co Ltd v Commission of the European Communities*[76] the Court noted that while the right to data protection might be a feature within the broader context of 'private life', as per the European Court of Human Rights, not all personal data inherently is measured 'private life'. This Court's line of thought may be grounded in the acknowledgment that certain facts about an individual, such as one's height, complexion and body build, inherently are part of public life simply by their existence.[77]

This article subscribes to the notion that privacy and data protection bear substantial yet distinct similarities. This stance is reached by recognising that issues related to data protection and privacy, to some extent, are practical considerations.[78] Essentially, the legal analysis of privacy and data protection must be conducted within the specific context in which they befall. Privacy is not a concept that can apply universally to different situations.[79] Solove's bottom-up approach involves conceptualisation of privacy by considering context-specific.

72 P de Hert & E Schreuders, *'The Relevance of Convention 108'* (2001) 33,42, Proceedings of the Council of Europe Conference on Data Protection, Warsaw, 19-20, November, 2001 cited in *'EU Study on the Legal Analysis of a Single Market for the Information Society'* (2009), Chapter 4, p.4.

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

74 As above.

75 LA Bygrave 'The place of privacy in data protection law' (2001) 24 *University of New South Wales Law Journal* 282.

76 *The Bavarian Lager Company Ltd v Commissioner of the European Communities* ECR T-194/04, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004A0194:EN:HTML (accessed 20 December 2021).

77 *Bavarian Lager Company* (n 76) 118.

78 Solove (n 51).

79 As above.

This means scrutinising privacy violations as disturbances of specific practices and regulations, such as interfering with peace of mind, intrusion on solitude, or loss of control over facts.[80] In examining the practices under the UBR, it is important to analyse whether in the context of the law, the UBR's practices offer a pragmatic response to data protection. Are there modern solutions for the potential problems created by the UBR?

7 Scope of data protection law in Malawi

7.1 Right to privacy under the Constitution as encompassing data protection

A discussion of enacted laws in Malawi arguably starts with reference to the Constitution of Malawi.[81] The rationale is that the Constitution is the supreme law.[82] Chapter IV of the Malawian Constitution contains provisions for human rights that must be respected and upheld by the branches of government. Additionally, these rights, where applicable, apply to all natural and legal persons in Malawi.[83] One of these rights is the right to privacy. Data protection can ensure that the right to privacy is safeguarded.

Section 21 of the Republican Constitution of Malawi provides for the right to personal privacy.[84] It provides as follows:

> Every person shall have the right to personal privacy, which shall include the right not to be subject to –
>
> (1) searches of his or her person, home or property;
> (2) the seizure of private possessions; or
> (3) interference with private communications, including mail and all forms of telecommunications.

In its enacted form, the section does not address the concerns of data protection. In this regard, it may be argued that there is a traditional conception of privacy under section 21 of the Malawian Constitution, which is not technology responsive.

Nyemba argues that section 21 of the Constitution is wide and may be interpreted to cover the right to privacy as also including the right of the individual to have their data protected.[85] This article agrees with the aforementioned observation. However, such wide interpretation would only

80 As above.
81 Republic of Malawi (Constitution) Act 20 of 1994.
82 As above.
83 Malawi Constitution (n 81) sec 15(1).
84 https://www.constituteproject.org/constitution/Malawi_2017#s166 (accessed 20 September 2023).
85 Nyemba (n 28).

be supported as a result of judicial pragmatism owing to the absence of a clear provision in the Constitution on the need to protect personal data. Regardless, by providing for the right to privacy, the article argues that section 21 of the Constitution encompasses data protection as the obligation therefore extends to data processors not to interfere with the privacy of individuals, owing to this constitutional right.

The right to privacy as it appears under the Malawian Constitution is coined in almost similar fashion with the provisions in article 12 of the Universal Declaration,[86] which proscribes arbitrary interference with a person's privacy and accords persons protection before the law against such interference. The Universal Declaration is enforceable as part of municipal law in Malawi.[87] The only differentiating feature with section 21 of the Malawian Constitution is that article 12 of the Universal Declaration appears to be narrow and limited.[88]

In December 2013 the United Nations General Assembly Resolution on the right to privacy in the digital age approved the General Comment of the United Nations Human Rights Committee on the right of privacy, family, home, correspondence, and protection of honour and reputation under ICCPR.[89] The General Comment calls for concise laws to protect the right to privacy, especially in the case of state surveillance and data processes.[90] To uphold the right to privacy, state parties must have precise laws in their surveillance activities, including the social protection sector such as the UBR. It is essential to ensure that individuals' privacy is protected, and clear laws can help achieve this.

General Comment 16 on the right to privacy, family, home and correspondence, and protection of honour and reputation (on article 17) of 1988, and General Comment 19 on the insurance of the family, the right to marriage and equality of spouses (on article 23) of 1990 hold significant importance in the realm of data protection.[91] These observations aim to address the gaps that emerged with the initiation of data protection discourse in the right to privacy sphere. They are crucial because they provide guidance on safeguarding personal data while protecting an individual's right to privacy. By emphasising the importance of protecting family, home, and correspondence, these General Comments highlight the need for privacy in all aspects of life, including the digital world.

86 Universal Declaration of Human Rights (Universal Declaration) adopted 10 December 1948.
87 The Universal Declaration is enforceable in the courts of Malawi as per *R v Chihana* (MSCA Criminal Appeal 9 of 1992) [1993] MWSC 1 (28 March 1993) where it was held that '[w]e accept that the UNO Universal Declaration of Human Rights is part of the law of Malawi and that the freedoms which that Declaration guarantees must be respected and can be enforced in these Courts'.
88 The same applies to art 17 of ICCPR.
89 Malawi is a state party to ICCPR having ratified it on 22 December 1993.
90 https://privacy.sflc.in/universal/ (accessed 3 January 2022).
91 C Kuner, *An International Legal Framework for Data Protection: Issues and Prospects', Computer Law & Security Review,* (2009), *Vol. 25, No.4, pp.307-317, at p. 308.*

General Comment 16 on article 17 of ICCPR acknowledges that the right to privacy is not only limited to its previous traditional conception. It is thought that General Comment 16 was passed because of the narrow framing of article 17 of ICCPR. Additionally, it may be argued that General Comment 16 augurs well with the principle of legal certainty which requires laws to be definite and clear. General Comment 16 is partly couched in the following terms:

> The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorised by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to, ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[92]

The effect of this General Comment is that the realm of data protection is placed under the wings of the right to privacy under ICCPR as well as the Universal Declaration. Section 211 of the Malawian Constitution provides for the legislative force of international law which Malawi.[93] It provides as follows:

(1) Any international agreement entered into after the commencement of this Constitution shall form part of the law of the Republic if so provided by an Act of Parliament.
(2) Binding international agreements entered into before the commencement of this Constitution shall continue to bind the Republic unless otherwise provided by an Act of Parliament.
(3) Customary international law, unless inconsistent with this Constitution or an Act of Parliament, shall form part of the law of the Republic.

Effectively, therefore, protection of personal data is provided for under the law in Malawi. The first reason is that Malawi has been a state party to ICCPR since 22 December 1993.[94] Since Malawi ratified ICCPR before the commencement of the Constitution, ICCPR is enforceable as part of domestic law.[95] The second reason is that section 11(2)(c) of the Constitution enjoins the courts to interpret the Malawian Constitution in line with international law norms, and that,

92 Human Rights Committee General Comment 16: Article 17 (Right to Privacy) The right to respect of privacy, family, home and correspondence, and protection of honour and reputation para 10.
93 https://www.constituteproject.org/constitution/Malawi_2017#s2234 (accessed 21 September 2023).
94 https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=104&Lang=EN (accessed 21 September 2023).
95 TT Hansen 'Implementation of international human rights standards through the national courts in Malawi' (2002) *Journal of African Law* 31.

therefore, the privacy provision under the Constitution may be interpreted in reference to General Comment 19.[96]

In this regard, it may be argued that based on section 21 of the Constitution and articles 12 and 17 of the Universal Declaration and ICCPR respectively, the requirement of data protection under the law subsists.

8 The Electronic Transactions and Cyber Security Act

The Electronic Transactions and Cyber Security Act 2016 (ETA 2016)[97] entered into force on 1 June 2017. It may be considered as the first major attempt to address data protection and privacy issues in Malawi. The long title to the ETA 2016 provides as follows:

> An Act to make provision for electronic transactions; for the establishment and functions of the Malawi Computer Emergency Response Team (MCERT); to make provision for criminalising offences related to computer systems and information communication technologies; and provide for investigation, collection and use of electronic evidence; and for matters connected therewith and incidental thereto.

As can be seen from the long title, the Act's objectives are diverse, as noted by Nyemba.[98] One of the objectives appears in Part VII which provides for data protection and privacy. Part VII is brief and is contained in four sections of the ETA 2016.[99]

Section 71 of the ETA 2016 outlines a data controller's responsibilities. A number of requirements are outlined in section 71(1) when handling personal data. Section 71(1)(a) stipulates that a data controller is obligated to guarantee that all data is processed lawfully and fairly. This is the first requirement. Second, section 71(a)(b) states that information must be gathered with specific, explicit and legal reasons in mind and cannot be processed in a manner that is inconsistent with those goals. Section 71(1)(c) establishes the minimal data dealing principle. Users of data must gather only information that is sufficient, pertinent, and not excessive in light of the reasons for which the data is being gathered and processed. Section 71(1)(d) lays down the fourth condition, which calls on data controllers to ensure that the data they collect is accurate and, if needed, kept up-to-date. Building on the necessity of maintaining accurate data, section 71(1)(e) mandates that data that is incomplete or wrong be erased or corrected in light of the reasons for which it was gathered or processed further. According to

96 Malawi Constitution secs 107 & 11(2) (c); R Kapindu J 'The relevance of international law in judicial decision-making in Malawi' Paper presented at the Judicial Colloquium on the Rights of Vulnerable Groups, held at Sunbird Nkopola Lodge, Mangochi, Malawi, 6 and 7 March 2014.

97 Cap 74:02 of the Laws of Malawi, 'Electronic Transactions and Cyber Security Act', https://malawilii.org/akn/mw/act/2016/33/eng@2017-12-31 (accessed 21 September 2023).

98 Nyemba (n 28).

99 ETA (n 97) secs 71-74.

section 71(1)(f), the data controller's last obligation is to retain data in a format that makes it possible to identify data subjects for as little time as is required for the purposes for which it was originally collected or for which it is subsequently processed. The right to be forgotten has anything to do with this. It mandates that data controllers retain information for as long as is required to fulfil the objectives for which it was gathered. One could argue that this criterion ensures that the hazards related to data storage are kept to a minimum.

The ETA 2016 allows for the processing of personal data in section 71(2). According to section 2 of the ETA 2016, processing of data includes any action or sequence of actions taken in relation to data, whether or not they are carried out automatically. These actions include gathering, logging, organising, storing, adapting or altering, retrieving, consulting, using, disclosing via transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying data.

A need for data processing is provided by section 71(2)(a), which states that processing of data is permitted only with the consent of the data subject. In this context, consent refers to the requirement that the data subject be informed of the intended data processing's aims and, as a result, that the consent comes from their free will.[100] Data processing is made possible by section 71(2)(c), which essentially enables a data controller to carry out his legal obligations. One instance of this would be if the authority sought reports from a data controller regarding the processing of data.

Subject data may also be processed under section 71(2)(e) if the processing is done in the public interest or in accordance with an official authority. According to section 71(2)(f), processing of personal data is allowed if it serves the legitimate interests of the data controller, a third party, or parties to whom the data is disclosed. However, in cases where the data subject's fundamental rights and freedoms are more important than these legitimate interests, processing of the data is prohibited.

It is evident from the aforementioned clauses that there are several restrictions on data processing. On the other hand, one could counter that the data controller has broad authority over data processing. In light of the diverse definition of data processing provided in section 2 of the ETA 2016, this point has been made. It is opined that the definition section should have included the definitions of the various components of the definition. In its current state, the data controller may perform various acts related to personal data and still fall under lawful data processing. An example of this relates to collection. The ETA 2016 does not expound on the prerequisites to lawful collection. Elsewhere, consent as related

100 ETA (n 97) does not define consent but rather provides what constitutes consent. This understanding, it may be argued, is guided by art 1(2) of the SADC Model Law on Data Protection.

to consent relates to freely-given, unambiguous consent. It further empowers the data subject to withdraw consent after having given it. It also mandates that data controller to keep a record of the permission.[101]

The rights of data subjects are outlined in section 72 of the ETA 2016. It gives the data subject the free right of access to their personal records about themselves without any costs to them. To verify whether their data is being processed, the data subject has access to it. The data subject has the right of communication on the processing, sources, and possible recipients of the subject's data according to sections 72(1)(a) and (b). A data subject may object to data processing under section 72(2) for valid reasons. There is a claim that doing so guarantees the data subject a remedy. The second remedy is for the data subject to request the rectification, erasure, or blockage of any data whose processing violates this Act's rules, particularly if the data is incomplete or erroneous. This need is consistent with General Comment 16 on article 17 of ICCPR and the obligations placed on a data controller in sections 71(1)(d) and (e), as previously stated, which demand accurate data.

Section 73 of the ETA mandates the data controller to notify the data subject of the name of the data controller or his representative, the purposes for which the data is collected, and the data subject's rights in order to enable the data subject to give informed consent.

Section 74 of the ETA 2016 is particularly significant as it mandates the data controller to put in place organisational and technical safeguards to protect personal data from unauthorised access, disclosure, alteration, and destruction – including accidental loss, theft and alteration – as well as from all other unlawful forms of processing, especially when the processing involves the transmission of data over a network. Therefore, section 74 protects data subjects' privacy by means of safeguards established by the controller, including protocols and other standard working documents.

9 Access to Information Act

Section 20 of the Access to Information Act (ATI) is of special relevance. It states that information concerning a third party must not be shared until it has been determined whether the information indeed is secret and whether disclosure would be damaging. Section 29 further states that personal information must not be provided in an unreasonable manner. It might be claimed that leaving the determination of when to share data or not to the information holder exposes the entire provision to misuse. Consent must be a fundamental tenet. Furthermore, it

101 General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR).

is suggested that the acts be linked with references to each other for consistency's sake. The other alternative route is to have a consolidated piece of legislation.

10 Informative international instruments and aspirations on data protection

10.1 General Data Protection Regulation

The General Data Protection Regulation (GDPR) is the data protection regulation of the European Union (EU). GDPR entered into force in 2016. By 25 May 2018 all organisations were mandated to be GDPR compliant. GDPR is applicable to member states of the EU. A salient feature of GDPR is that it also has extraterritorial application in that data processors may fall under the purview of GDPR so long as the data subjects that are targeted and/or the data that is collected relates to people in the EU.

Of particular interest in GDPR is article 5. It guides principles that should guide personal data processing. There is a total of seven principles. The first is the principle of lawfulness, fairness and transparency. It entails the need to process data in circumstances that are permitted by law, based on fair considerations and in a manner that is sufficiently transparent. The transparency, it may be argued, should involve the data subject as the centre piece of data processing. It could also involve putting in place mechanisms that safeguard the right of access and information to the data processing by the data subject where possible.

The second is purpose limitation. This principle requires that data is collected for specified, clear and valid purposes. Consequentially, therefore, data must not be processed for any other means that are incompatible with the purposes for which it was initially collected. Nonetheless, there is a caveat in that data collected for other purposes may be further processed where the public interest so demands, or where research purposes for historical, scientific or statistical ends may so require. This, in line with article 89(1), is not to be considered incompatible with specified purposes for which the data was initially collected.

The third principle under article 5 of GDPR is data minimisation. This principle is brief. It requires that data should be only sufficient for the purposes for which it is collected, relevant and limited to those purposes, as much as necessary.

The fourth principle is accuracy. Data should be accurate in relation to the 'actual' data subject and that, where necessary, data processors must put in place mechanisms that ensure that the data is up-to-date. Any inaccuracies must be rectified or erased without delay.

Storage restriction is the fifth principle. In accordance with the purpose restriction principle, this concept mandates that data storage that identifies the data subject be kept for no longer than the period of the reasons for which it was obtained. The exception is processing for archiving purposes which, as stated in article 89(1), does not contradict the reasons for which data is gathered. As a result, the same may apply to the length, as long as the archiving is for the objectives specified in the discussion of purpose restriction. This exception, however, is subject to the execution of the relevant technological and organisational measures required by the rule to protect data subjects' rights and freedoms.

The final but one principle is the integrity and secrecy principle. The essence of this concept is the requirement to safeguard personal data through suitable technological and organisational safeguards. Among other things, the procedures should strive to avoid illegal data processing, inadvertent data loss, and unauthorised access.

The final element is accountability, which requires the data controller to be accountable and demonstrate compliance with the six criteria listed above.

GDPR is also praiseworthy for granting data subjects additional rights. These include the right to information; access; rectification; erasure; restriction of processing; data portability; and objection to processing. This article will not go into further depth on these rights as it is slightly outside the scope of the article.

10.2 African Union Convention on Cyber Security and Personal Data Protection

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) was accepted on 27 June 2014 during the AU Assembly's twenty-third ordinary session in Malabo, Equatorial Guinea. It currently has only been signed by 16 nations, approved by 13 countries, and lodged by 13 countries.[102] Malawi is not a state party to the Convention. Problems of non-domestication are not alien. Various reasons, such as the domestication process, have been proffered. For example, the AU Report on Malawi's non-compliance with its protocols and charters notes as follows:

> The limited domestication of international protocols, including those of the African Union, is considered to be largely a result of [Malawi's]domestication system. While the exclusion of Parliament from the ratification process ensures a relatively speedy process of ratification, the main drawback is that in the long run, law-makers (Members of Parliament) are less aware of the instruments that the country is a

102 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection (accessed 4 January 2022).

signatory to or not. As a result, the National Assembly is not in a position to make reference to them when debating legislation.[103]

Malawi's non-ratification of the Malabo Convention may only be speculated upon, but the reasons noted in the above report may be relevant.[104]

Article 11 of the Malabo Convention requires governments to establish a self-governing administrative entity entrusted with protecting personal data. Article 12 of the Convention requires nations to impose restrictions on the processing of personal data, including restrictions based on public interest and storage. One of the primary shortcomings of the Convention is that it does not define lawful data processing. Ball has also identified this as a significant component of the Convention that may expose data processing to the data controller's subjectivity.[105]

One of the Malabo Convention's significant innovations is the notion of consent. According to article 1 of the Convention, consent is the expression of a definite, explicit and informed will with regard to the data that a data processor requests to handle. The permission might come from the data subject themselves or from their legal, judicial or treaty representative.

10.3 The SADC Model Law on Data Protection

2013 saw the adoption of the SADC Model Law on Data Protection, which was created in 2010. The goal of the member nations is to protect personal information. The goal of this regional endeavour is to guarantee data privacy for all member states in the area. Similar to the Malabo Convention, the Model Law's definition of consent is one of its most notable features. Consent is defined under the SADC Model Law in the same way as the Malabo Convention.[106] The central piece of this definition is the need for clear consent on the part of the data subject. Part III of the Model Law also provides for a data protection authority tasked with regulatory powers for data protection. This is a good innovation as it provides for a specialised authority to carry out supervisory powers to ensure data protection.

Under the SADC Model Law, the processing of personal data is subject to the same requirements as under GDPR. Thus, it can be observed that the Model Law only followed the EU legal framework's data processing methodology. On the other hand, the SADC Model Law deserves praise for focusing specifically on the handling of private information. It forbids the processing of sensitive personal

103 'Malawi's compliance with African Union charters and protocols' State of the Union, AU, 2015.
104 As above.
105 K Ball 'Introductory note to the African Union Convention on Cyber Security and Personal Data Protection' *International Legal Materials* 1, <DOI: https://doi.org/10.1017/ilm.2016.3 (accessed 20 February 2022).
106 SADC Model Law on Data Protection art 1(2).

data that might expose the identities of the data subjects, thereby putting them at greater risk.[107] However, if a data subject provides consent, the data may be processed in accordance with the legal provisions that allow for such consent to be granted.[108]

The ETA 2016 and the data controller's responsibilities are nearly identical, with the latter requiring the former to inform the former about the processing of the subject's personal data.

Organisations must also include organisational and technical safeguards against unintentional access, careless erasure, destruction or alteration, according to the SADC Model Law.[109] The SADC Model Law's article 31 gives data subjects rights regarding data controllers. In essence, the person whose data is being processed has control over the actions taken with respect to that data. In summary, the SADC Model Law indicates a strong regional aim for the protection of personal data and presents a complete strategy.

The major drawback of the Model Law is on the remedies and rights of data subjects. Literacy levels may militate against the illiterate accessing remedies that require written notices. Additionally, the Model Law does not make provision for decentralisation or mobile operations of the data authority to ensure that even the poor are reached and have access to remedies under the law.

11 Personal data protection under the Universal Beneficiary Registry

11.1 Protection of personal data under the UBR

A number of the UBR Protocols' clauses are designed to protect personal information. The requirement for consent before processing data is the main one. Section 71(2)(a) of the Electronic Transactions and Cyber Security Act is in compliance with this requirement. The UBR Protocols provide a number of noteworthy data protection features. For example, they mandate all personnel – employees, contractors, consultants and visitors – to acquire knowledge of the information security policies, guidelines, processes and mechanisms, and they also have a responsibility to secure the UBR's information assets. Additionally, accessing or using UBR assets without permission from the UBR management team is prohibited by the UBR Protocols.

107 SADC Model Law on Data Protection Part V, art 15.
108 As above.
109 SADC Model Law on Data Protection art 24.

It is necessary to notify the UBR administrator of security breaches that could expose data to unauthorised dissemination. The rules specify that a failure to familiarise oneself with the UBR's security standards will not be accepted as an excuse, presumably in an effort to ensure that all staff members handling UBR data understand them.

It is necessary to notify the UBR administrator of security breaches that could expose data to unauthorised dissemination. The rules specify that the failure to familiarise oneself with the UBR's security standards will not be accepted as an excuse, presumably in an effort to ensure that all staff members handling UBR data understand them.

Furthermore, handling data on personal and portable devices is forbidden by the UBR Protocols. It is believed that this lowers the possibility of loss that accompanies the carrying around of portable electronics. Furthermore, data users must set up safeguards to protect the confidentiality and integrity of personal data in accordance with UBR Protocol Section 3.1.1(h). One could argue that this obligation imposes a fiduciary duty on data users to behave in the subjects' best interests. The Protocols demand special vigilance when handling printed extracts of shared UBR data as data may also be stored in hard copy format.

The above requirements agree with the provisions of section 74 of the ETA which provides as follows:

> (1) A data controller shall implement technical and organisational measures enabling to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
> (2) Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Five primary security goals are identified by the UBR under Part 4 of the UBR Protocols. 'Security obligations' appear in the marginal notes of section 74 of the ETA. The UBR's security objectives are intended to help it fulfil its security-related responsibilities. The UBR's primary security goal is 'availability'. It implies that there must be enough security measures in place to guarantee recoverability in the case of an interruption and that the personal data stored there is accessible to authorised users, clients and business partners when needed.

The second security objective is 'integrity and competence'. This objective aims at ensuring that the information held by the UBR is accurate and complete as far as necessary during the entire information processing cycle. This objective arguably stems from section 74 of the ETA above but is also in agreement with section 71(1)(e) of the ETA which requires accuracy of data.

'Confidentiality' is the third security goal under the UBR Protocols, and it calls for sufficient safeguards or controls to guarantee that information is only given to or made available to authorised processes, entities or individuals. The Constitution's section 21 guarantees the right to privacy. When those providing data do so, they do so solely to fulfil the objectives of the data collection. Therefore, it is important that such data be kept private and used only for those purposes after it has been gathered.

The fourth security objective under the UBR Protocols is 'authenticity', which requires adequate controls or safeguards to be in place to uniquely identify users of information assets to the information being accessed. This security objective is in line with section 74 of the ETA, which charges data controllers to put in place technical and organisational measures to safeguard data. In this regard, the security objective charges data users of the UBR framework with responsibility for the information which they access. In other words, the UBR management team seeks to achieve certainty that the partners they are dealing with are legitimate players in the social support strengthening programmes who may be held accountable for their actions.

The last security objective under the UBR Protocols is 'accountability'. It enjoins data controllers to be responsible for the data that they process, and to be accountable for their actions. This further means that the data controllers must adopt deliberate safeguards to ensure that any single controller is responsible for the data they process and their actions in relation to the same. Data controllers and users exercise their functions on the basis of trust. It is only pertinent that they should be held accountable for their actions.

11.2 Adequacy of data protection under the UBR

To a larger extent than not, the UBR Protocols have attempted to offer data protection. However, as was already mentioned, privacy primarily is the responsibility of the data subject, who aims to limit the amount of personal information that may be made public. Nevertheless, an examination of the UBR Protocols has shown that the topic of the data is only mentioned in passing. The 29-paged Protocols contain two instances of the term 'data subject'. It is crucial that the information that data processors have about a data subject is centred around them.

The ETA's section 73 grants the data subjects a number of legal rights. The first of these is the right to know the identity of the data controller and the reasons behind the collection of personal data. The right to object is the last and, possibly, most important right of the data subject. For valid reasons, one may object to the processing of personal data. The information processing may cease to involve a particular data subject in the event that the data subject raises an objection. The requirement that any such objection be supported by a valid

argument is a restriction, nevertheless. Finally, a data subject has the right to request, from a data controller, the correction, erasure or blockage of data of which the processing violates the Act's requirements, particularly where the data is erroneous or incomplete.

Although certain rights fall within the recently-described requirements, they do not grant the data subject a direct right of action against the data controller, which includes the UBR, data users and/or third parties. In this context, one could contend that the rights granted to the data subject by the ETA are of a remedial character. According to the opinion, if the same had been ingrained in the procedures, they would have been procedural and would have given a data subject greater certainty regarding the protection of their privacy.

Additionally, the UBR Protocols are contractual in nature. In general, they cover the agreement between data users and data controllers. By their legal nature contractual arrangements are between the parties to such an arrangement. It is trite, therefore, that rights and obligations under such arrangements are a matter of principle between the parties. The sobering thought is the recourse that a data subject has against a third party that might have illegally accessed their personal information. This would occur even where the data user has undertaken all contractually-necessary steps.

Under part 8 of the UBR Protocols, to protect the privacy of data, the only provision dealing with third parties cautions against data sharing with third parties. It declares that if data is shared with unaffiliated parties, the data user will be held accountable and subject to legal consequences. As much as is it realistic that data may be exposed to third parties, this poses a potential challenge for a violation of rights of data subjects. However, there are remedies in the law as observed in the UBR Protocols, such as section 84 of the ETA which deals with unauthorised data access by third parties.

12 Concluding remarks: Personal data protection in Malawi

The Electronic Transactions and Cyber Security Act represented Malawi's most significant attempt to address data protection issues.[110] The Act is both a civil and penal legislation. The ETA defines personal data as any information about an individual that could be used to directly or indirectly identify that specific individual via the use of different aspects.[111] Section 3 of the ETA provides for the objectives of the Act. Section 3(a)(ii) provides that one of the objectives is to balance societal and individual interests in the exploitation of information. Section 3(c) provides a further objective, which is to ensure that there exist proper mechanisms to ensure data protection, among others. Section 3 of the

110 ETA (n 97).
111 ETA (n 97) sec 2.

ETA makes it clear that the Act's responsibility is to safeguard data subjects' personal information.

The Malawi Communications Regulatory Authority is tasked with implementing the ETA in accordance with section 5. The Act, however, is silent about a data protection authority. The Act does not provide for the appointment of a data protection authority, in contrast to other sections, such as section 6, that establishes the Malawi CERT, and section 75 that appoints the domain registrar in charge of managing the .mw domain.

The statute appoints a data protection authority to manage data protection issues, following international legislative practice. Part III of the SADC Model Law on Data Protection, for example, establishes a data protection authority. According to the SADC Model Law, one of the persons tasked with ensuring that the controller's data processing conforms with the law is the authority.[112] As mandated by the SADC Model Law, the authority is also responsible for creating subsidiary laws in the form of rules that are enforceable statutory instruments.[113] Other provisions under article 4 of the SADC Model Law entitle the authority to make enquiries of its own accord or after having received complaints, into data protection issues. The authority under the SADC Model Law is also to be empowered to receive complaints by various means.

This is where the Electronic Transactions and Cyber Security Act's legislative approach falls short. According to this research, it would resemble carrying water in a leaky bucket to lay out the obligations of data controllers and the rights of data subjects without a framework to enforce them. The Act makes no mention of any protective authority's responsibilities.

Nonetheless, the Malawi Communications Regulatory Authority, as earlier presented, is tasked with implementing the ETA. In this regard, the MACRA Board may simply establish a directorate of data protection. However, this may be undesirable and with less effect as the directorate is not directly provided for under the Act. Therefore, it is believed that the appropriate course of action in this case may be to create specific provisions under part VII of the ETA that explicitly grant MACRA – referred to as the authority under section 2 of the ETA – the right to adopt the SADC Model Law's framing and give it the explicit authority to create regulations for the protected privacy and data. Alternatively, as in other statutes, the Act may specify the authority's functions.[114] The advantage of this is that it achieves one of the law's desirable qualities, which is certainty.

112 ETA (n 97) art 4(1)(a).
113 ETA (n 97) art (1)(d).
114 Eg, Cap 48:09 of the Laws of Malawi, 'Competition and Fair Trading Act,' clearly spells out the functions of the Competition and Fair Trading Commission under sec 8.

Establishing data protection authorities is a requirement of the African Union Convention on Cyber Security and Protection of Personal Data for state parties.[115] In contrast to the SADC Model Law, the AU Convention stipulates that the data protection authority must be an independent body.[116] Given that MACRA also performs other legal duties unrelated to data protection, it would be considered inappropriate for data protection purposes in this regard.

However, it is opined that having MACRA to be the authority would assist Malawi in saving resources. This is because new staff recruited would share infrastructure and other economic resources with an already-established system. Establishing an independent authority would mean an extra board for the government. This research is of the view that the legislative approach under the ETA with regard to the authority responsible for data protection fits our economic realities. On the other hand, the benefits of an independent authority are that there would be a concentration of expertise, unlike if data protection were regulated by a non-specialist authority whose board is diversely drawn.

The government should consider ratifying the AU Convention on Cyber Security and Personal Data Protection, as its provisions for a data protection authority are precise and appear to align with Malawi's social, cultural and economic conditions.

12.1 The Draft Data Protection Bill

Malawi's intentions and goals for a data protection framework are reflected in the Draft Data Protection Bill. For the purpose of comparative legal analysis, the Data Protection Bill is discussed. One of the objectives of the research was to conduct a comparative law analysis. It is only pertinent that the legislative aspirations are measured against comparable law to better understand whether the approach taken has the potential of safeguarding personal data under schemes such as the UBR.

The 2021 Draft Data Protection Bill's lengthy title states that it is an Act to make provision for protection of personal data, for regulation of the processing of personal data, and for matters connected therewith or incidental thereto.

The Malawi Communications Regulatory Authority will continue to be the body responsible for safeguarding personal data, which is the first noteworthy aspect of the Data Protection Bill. The Draft Data Protection Bill's intentions are explicit, in contrast to those of the ETA. For example, section 3's goals include ensuring that processing personal data conforms with data protection standards,

115 African Union Convention on Cyber Security and Protection of Personal Data art 11.
116 African Union Convention on Cyber Security and Personal Data Protection (n 88)

such as privacy and data security.[117] Additionally, the Bill aims to protect data subjects' rights regarding the handling of their personal information.[118] The fact that the Bill also aims to control cross-border transfer of personal data is one of the noteworthy introductions to the discussion of data processing in Malawi. The law did not specifically provide for the protection of personal data with relation to cross-border transmission under the former system, primarily part IV of the ETA.

Section 5 of the Draft Data Protection Bill is noteworthy as it provides an exemption from processing personal data obtained for home, recreational or personal purposes. Given that the data subject's rights are still at risk, the research has not been able to understand the justification for such an exemption. For example, it would be problematic if a leisure club that gathers member data was discovered to have violated the Act and then allowed to continue operating without consequences.

Additionally, the Draft Data Protection Bill keeps MACRA as the body in charge of putting it into effect.[119] In section 8 it states that MACRA, the authority, would have a data protection unit. Thus, the section 5.2 explanation of the data protection authority's independence is applicable here, *mutatis mutandis*. According to the research, an independent data protection authority is recommended for the previously-mentioned reasons.

The principles for data processing are provided for in section 18 of the Draft Data Protection Bill. The ETA, the SADC Model Law and the AU Convention on Cyber Security and Data Protection are all reflected in the guiding principles. Based on the research, it is concluded that the data processing principles should be adhered to in terms of methodology. The principles protect data subjects' rights in accordance with section 21 of the Constitution, which protects data subjects' privacy through the right to privacy. However, these principles are the same as those provided for under section 71(2) of the ETA. It therefore does not make much legislative sense to have provisions in two Acts of Parliament that mirror each other. It is opined that the provisions in the ETA regarding data processing should, therefore, be repealed once the Data Protection Bill enters into force.

The issue of data protection pertaining to children is also included in the Draft Data Protection Bill. It stipulates that a legal guardian's consent is required.[120] This is a welcome approach as the previous regime did not address the issue of data privacy for minors.

117 Draft Data Protection Bill sec 3(a), https://digmap.pppc.mw/wp-content/uploads/2022/03/Malawi-Data-Protection-Bill-final-draft-210630-.pdf (accessed 22 September 2023).
118 Draft Data Protection Bill (n 117).
119 Draft Data Protection Bill (n 117) sec 6.
120 Draft Data Protection Bill sec 20.

It is believed that if the Bill is approved by the legislature, the legal protection of personal information will be enhanced. As a result, programmes such as the UBR that protect personal data will be protected.

13 Implications of Malawi's Current regulatory framework on the UBR data-sharing framework and personal data protection

Administrative remedies for breaches of personal data are not provided by the Protocols, as was mentioned during the UBR's examination of the data protection framework. For this reason, section 35 of the Draft Data Protection Bill is relevant. It offers guidelines by which a data controller can be considered to provide sufficient data protection. A few of these are the existence of legally-binding rights for data subjects, their capacity to seek judicial or administrative recourse to protect their rights, and the rule of law in general.[121]

It was noted that data sharing under the UBR is contractual in nature. One of the challenges noted with this arrangement was the security objective of authenticity of the data user. However, since section 37 of the Draft Data Protection Bill mandates data users' registration, this issue might be resolved.

The following are some ways in which the current legislative framework affects the UBR and personal data protection: The Constitution and part VII of the ETA do not fully guarantee the right to data protection. Since the SADC Model Law on Data Protection and other instructive international documents are in line with regional ambitions, it is vital that the UBR data sharing framework implement procedures for the protection of personal data at all times. Respecting section 71 of the ETA's data processing guidelines is another aspect in this regard. Section 74 of the ETA requires the UBR data-sharing framework to establish adequate organisational and technical safeguards for the security and protection of personal data. However, in situations where there has been a breach of a data subject's personal information, the existing legal system does not offer the data subject primary remedies. It is argued that this could have a detrimental effect on the safeguarding of personal data because the legal system's redress procedures could be expensive and time-consuming.

The significance of a person's right to privacy has been highlighted in the article. Its primary focus was on the risks associated with the information society's gathering of personal data. Among the numerous risks are security lapses, illegal access, loss and erasure. The goal of the study was to establish how Malawian legislation protects the protection of personal data. It was discovered that Malawi has laws designed to protect personal information. The Electronic

121 Draft Data Protection Bill sec 35(2)(a).

Transactions and Cyber Security Act is one of the most notable of these. Ultimately, nevertheless, it was determined that the statute lacked the necessary comprehensiveness. Comparable laws, such as the AU Convention on Cyber Security and Data Protection, the General Data Protection Regulation and the SADC Model Law on Data Security, provided lessons throughout the research. As a result, it was suggested that the law should move closer to enacting an extensive data protection framework.

The study then looked into Malawi's actual practices for protecting personal data. A case study utilising the Unified Beneficiary Registry was conducted. According to the study's findings, the UBR had implemented organisational and technical safeguards to protect data subjects' personal information. Nonetheless, it was discovered that the UBR Protocols' most significant flaw was their failure to provide for data subjects' administrative rights. However, it was determined that the UBR provides reasonable safety for personal data.

The article's emphasis was redirected to data protection legislation processes, specifically focusing on the Draft Data Protection Bill. The investigation came to the conclusion that the UBR data-processing procedures are affected in a number of ways by the Draft Data Protection Bill. The requirement that data users register with the authority is one of these. The Draft Bill also mandates the use of administrative measures to protect the rights of data subjects.

The study further is of the view that the data protection authority in Malawi should be an independent body responsible for enforcing data protection laws.

In essence, the study's conclusion about Malawi's legislative procedures is that the country should take a comparative approach rather than attempting a wholesome adoption of regional and international data protection laws.

African Journal on Privacy & Data Protection

To cite: AO Salau 'Cybersecurity, state surveillance and the right to online privacy in Nigeria: A call for synergy of law and policy' (2024) 1
African Journal on Privacy & Data Protection 152-175
https://doi.org/10.29053/ajpdp.v1i1.0008

Cybersecurity, state surveillance and the right to online privacy in Nigeria: A call for synergy of law and policy

*Aaron Olaniyi Salau**
Reader in Law, Faculty of Law, Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria
https://orcid.org/0000-0002-6703-7794

Abstract:

As presented in this article, the conditions of mutual dependence and interactions between cybersecurity and state surveillance equally pose risks to the right to online privacy (also referred to as 'internet privacy') regarding the collection, use, access and protection of personal data by the individual and the state. While cybersecurity measures are necessary to safeguard against threats to computer networks and public infrastructure and prevent identity theft, these must not become a subterfuge for unlawful surveillance and interference by the state with personal data. Indeed, the right to online privacy is protected internationally, and among the cluster of privacy rights guaranteed in section 37 of the amended Constitution of the Federal Republic of Nigeria 1999. The right protects personal data contained in communications and metadata but extends also to communication infrastructure and software systems that are increasingly being required to have in-built privacy and data protection controls in their design for better protection of personal information. Conversely, wide-ranging laws and policies enable the state to intercept and monitor internet and electronic

* LLB (Hons) LLM (OAU, Ile Ife) BL (Lagos) PhD (Cape Town); aaron.salau@oouagoiwoye.ed.ng

communications in disregard of personal privacy to uphold cybersecurity interests. Interestingly, the recently-passed Nigeria Data Protection Act 2023 has now set the required standards for data protection and privacy. Consequently, this article aims to determine the extent to which the right to online privacy is respected and may be restricted in Nigeria for state security reasons, including cybersecurity, and whether these accord with online privacy and data protection standards. Using the lens of liberal democratic theory to re-orientate the normative framework for privacy for the internet age, the article conceptualises the imperative of online privacy in the age of cyber (in)security and undertakes doctrinal scrutiny of international human rights instruments, particularly the African Union Convention on Cyber Security and Personal Data 2014, and relevant literature. The article recommends that the Nigeria Data Protection Act 2023, which was passed to domesticate the AU Convention on Cyber Security, be rigorously enforced, the national security exemptions applicable thereto must be spelt out from the inception while the adjustments necessary for its smooth implementation must be made to ensure data protection and privacy.

Key words: cybersecurity; Data Protection Act Nigeria; personal data; state surveillance; right to online privacy

1 Introduction

Internet-enabled computer networks, information and communication technology (ICT), and social networking platforms that enable the digital transmission of information in real-time have become indispensable for cost-effective access to public, social and commercial services. This increased dependence on the internet and ICT is based on a capitalist business model that requires the surrendering and processing of vast amounts of personal information of individuals (data subjects) that may be searched, aggregated and cross-referenced.[1] The latter allows for the commercialised sharing and dissemination of data, the systematic monitoring of the citizens' communications by service providers and the yielding of access thereto to the government by tech giants without the data subject's prior consent. The availability of public services on the internet also comes with increased threats of attack on critical infrastructure from hacktivists, internet fraudsters, terrorists and other cyber criminals which can endanger the national interest. Countering such threats against computer networks is achieved through cybersecurity policies/strategies that serve to justify data retention laws and 'dataveillance', which pertains to data-intensive surveillance technologies that monitor human behaviour, digital communications and online activities.[2] Consequently, the traditional conception of privacy as the ability to control

1 D Boyd & K Crawford 'Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon' (2012) 5 *Information, Communication and Society* 662, 663.

2 E Luiijf and others 'Nineteen national cyber security strategies' (2013) 9 *International Journal of Critical Infrastructures* 3, 5-8.

access to personal information, which protects human dignity and autonomy, becomes challenging in an atmosphere of mass surveillance and availability of 'Big Data'. In modern democracies based on the rule of law, any government intrusion on privacy calls for the legality, legitimacy and proportionality of such measures and the principled protection of informational privacy. In Nigeria, the challenge is that despite the pervasive incidents of cybercrimes in the country, the uncoordinated state of law and policy on cybersecurity seriously limits the enjoyment of online privacy. Consequently, the article explores the importance of democratic theory and the nature of reforms required to stimulate synergy between cybersecurity and privacy protections in Nigeria. Part 2 examines the principles of a democratic theory to guide the protection of online privacy in the cyber (in)security age. Part 3 expounds on the imperative of international human rights law and the African Union (AU) Convention on Cyber Security and Personal Data 2014 for online privacy protection. Part 4 examines the merits of the recently-enacted Nigeria Data Protection Act, 2023 in order to address the gaps in Nigeria's legal framework on online privacy and discusses how the theoretical framework developed in part 2 can inform the cybersecurity policy related thereto. Concluding, part 5 proposes legal and policy reforms to enhance online privacy and cybersecurity in Nigeria.

2 A democratic theory of privacy and cybersecurity

This part of the article develops a theory inculcating principles of online privacy that should guide the regulation of cybersecurity and inform the law on state surveillance in a democratic polity. To flesh out the theory, it is argued that the traditional conception of privacy as a private space of inviolate personality or self-identity based on the exercise of control, dominance or authority over personal information has become outmoded due to the impact of the internet on human activities. In the internet age, this yields a normative understanding of privacy beyond the private/public dichotomy due to the expanded opportunities for state surveillance in the name of cybersecurity measures to safeguard computer networks, public infrastructure and personal data against threats. This lends weight to the right to online privacy which offers a counterpoint to pervasive surveillance in the Internet age. The right serves to constrain mass surveillance of the citizens in view of the expansive meanings that are being ascribed to cybersecurity by both democratic and authoritarian governments. The notion of a private realm involving intimacy, secrecy, solitude or seclusion is of great social value, which is innate to human beings, although this has varied across cultures, civilisations, and historical and legal traditions.[3] Privacy is a reasonable and legitimate expectation of non-intrusion in all societies that enables every person or group to live a life free of patronising, paternalistic or meddlesome influences by others. Privacy is equally required to develop and nurture intimate,

3 S Gutwirth *Privacy and the information age* (2002) 24-26.

familial and other interpersonal relationships in a dignified manner even within public and private spaces.[4] Privacy thus is a multidimensional but much-interrogated concept as it can protect a person's bodily integrity, private life, home and communications from unwarranted searches and seizures and help to uphold one's life choices, reproductive autonomy, and so forth.[5] Nonetheless, the legal protection of privacy is one of the essential conditions for the furtherance of a free and democratic society, a means for the development of the human personality and enjoyment of civil liberties. The right to online privacy, which is the totality of the legal procedures, processes and systems available to protect one's personal information/data from unauthorised access, use or interference in the online environment, can be said to be an extension of this right.[6]

Classical expositions on the right to privacy see it foremost as evoking concerns over the control of personal information. Westin calls it 'the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others'.[7] Westin identified four 'basic states of individual privacy': (i) solitude; (ii) intimacy; (iii) anonymity; and (iv) reserve.[8] In this way, the expectation of privacy that a person has can be in terms of restriction: of intrusion by government agents; of access to sensitive, intimate, or confidential information; and into private spaces. Hence, the right to privacy is a value of much purchase in free and democratic societies due to the role it plays in limiting government's power over the citizens.[9] In their 1890 seminal article on privacy, Warren and Brandeis view privacy as the 'right to be let alone' based on the exegesis of the United States Constitution and Bill of Rights which, to a significant extent in the digital age, now includes the 'right to be forgotten'.[10]

Privacy also is a requirement for maintaining human agency, personhood or individual autonomy and consequent human flourishing in an atmosphere of dignity.[11] Autonomy in this context denotes the assertion of control over personal information relating to preferences, goals, aspirations, tastes, commitments, and so forth, which a person has cultivated over time ably assisted by zones of 'relative insularity' and uninhibited by traditions and conventions. The latter is the mark of a liberal citizenship defined by critical reflection over personal choices.[12] Furthermore, privacy provides the condition and ingredient to critical reflection

4 As above.
5 DJ Solove 'A taxonomy of privacy' (2006) 154 *University of Pennsylvania Law Review* 477, 549-550.
6 JE Cohen 'What privacy is for' (2013) 126 *Harvard Law Review* 1919.
7 AF Westin *Privacy and freedom* (1967) 31-32.
8 Westin (n 7) 33-36.
9 H Nissenbaum 'Privacy as contextual integrity' (2004) 79 *Washington Law Review* 119, 128-129.
10 A Forde 'Implications of the right to be forgotten' (2015) 18 *Tulane Journal of Technology and Intellectual Property* 83, 120.
11 B van der Sloot 'Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of big data?' (2014) 5 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 230, 234.
12 J Cohen 'Examined lives: Informational privacy and the subject as object' (2000) 52 *Stanford Law Review* 1373, 1424; Nissenbaum (n 9) 148-149.

required for active citizenship, which is the participation in activities and discussions concerning political and other issues of general interest. This is because the citizens' ability to reach out to one another on matters of common interest may only be fully realised under an atmosphere free of an overbearing government. Similarly, privacy is an enabler and key condition for the enjoyment of freedom of expression and journalistic freedom, to mention but a few democratic rights.[13] For instance, those who provide information that journalists have a duty to publish do so on the basis of confidentiality. Journalistic freedom would be seriously hampered if the government were to force journalists to reveal their sources of news and information.[14] Contrariwise, freedom of expression itself would be 'chilled' if journalists become subject to reprisal attacks from persons who would otherwise wish that information that the public is entitled to receive be kept secret. From the foregoing, it may be safe to surmise, albeit at first glance, that aside from the need to protect individual interests, the collection and processing of personal or private information could also serve to protect countervailing collective values of a liberal democratic order such as national security, which may implicate the need for trade-offs and balance.[15] However, a binary conception of privacy that produces a static stimulus on the development of personhood or autonomy has become outmoded in the internet age as the concept always yields itself to varied changing contexts in which personal information is externally observable.[16] Moreover, Cohen observes that even in modern democracies, the internet has become a principal means of expression, information dissemination, and behavioural modulation.[17] As Rengel posits, considering that spaces for the expression of privacy shift and expand in response to innovations in information and computing and other internet-enabled technologies, the challenge then is how and to what extent a person's online privacy can be protected.[18] Nissenbaum thus argues for an approach to privacy regulation that considers the social context whereby data collected in a private setting ought not to be appropriated for public (online surveillance) purposes.[19] Surveillance could then ordinarily not be conceived as pernicious but as a public good and a means for social control and effective governance in which citizens, governments, businesses and other organisations have vested interests.[20] Furthermore, technological cybersecurity measures could also serve to protect the individual's data-based (digital rights) and personal data from being violated through cyber-attacks and, in turn, be complemented by data protection measures for privacy protection. This

13 'The right to privacy in the digital age' 71/199 (2017) UN General Assembly Resolution.
14 UNESCO 'The right to privacy in the digital age', https://www.ohchr.org/sites/default/files/documents/issues/digitalage/reportprivindigage2022/submissions/2022-09-06/CFI-RTP-UNESCO.pdf (accessed 31 March 2023).
15 Nissenbaum (n 9) 151.
16 Nissenbaum (n 9).
17 JE Cohen 'Surveillance vs privacy: Effects and implications' in D Gray & SE Henderson (eds) *Handbook of surveillance law* (2017) 455-469.
18 A Rengel 'Privacy as an international human right and the right to obscurity in cyberspace' (2014) 2 *Groningen Journal of International Law* 36, 41.
19 Nissenbaum (n 9).
20 AS Elmaghraby & MM Losavio 'Cyber security challenges in smart cities: Safety, security and privacy' (2014) 5 *Journal of Advanced Research* 491, 493-494.

should factor-in 'the right to [online] privacy as a necessary component in the development of a citizen-centric security policy'. The legal regime of 'cyber privacy' could therefore be accentuated by related statutory or regulatory prohibition of interference with, disruption or unauthorised access to a computer network, information system and related data or the unauthorised processing, interception or transmission of data.[21] However, 'cybersecurity' has no fixed definition but varied approaches. The International Telecommunications Union has defined cybersecurity as 'the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organisation, as well as users' assets'.[22] Cybersecurity could be said to relate to the practices and tools devised to ensure the confidentiality, integrity, and availability (the 'CIA triad') of computer systems and networks.[23] Also, cybersecurity involves the technical protection of the internet and ICT systems, the development of organisational and institutional capability by states to prevent and detect illegal cyber activity, and policy and legal measures to safeguard users against cybercrimes and the unauthorised use or appropriation of personal data.[24] Nonetheless, cybersecurity attracts cyber surveillance.[25] Democratic states have often used the growth in the various international dimensions of cybercrimes and cyber-attacks to justify the warrantless surveillance of citizens in the name of national security but with less concern for privacy.[26] Anticipatory surveillance of online activities by security agencies may be meant to detect, deter and counter the threats to national security in real-time, but its mass surveillance and data interception methods violate the dignity of persons with no criminal involvements and are discriminatory of individuals and groups thereby profiled.[27]

Furthermore, the interconnectedness of individuals and institutions in cyberspace and the role of technology in shaping human behaviour and the understanding of privacy cannot be overemphasised in exposing the power dynamics between individuals and the state. To reduce the ensuing asymmetric relationship, a way forward is that cybersecurity must be moderated by judicial and technical solutions.[28] Technological advancement has also opened

21 As above.
22 See ITU High Level Experts Group (2008), ITU Global Cyber-Security Agenda (GCA) High Level Experts Group (HLEG) Global Strategic Report, Geneva: ITU, 27.
23 AM Matwyshyn 'Cyber!' (2018) 2017 *Brigham Young University Law Review* 1138-1139.
24 National Initiative for Cybersecurity Careers and Studies 'Glossary' (2017), https://niccs.us-cert.gov/glossary (accessed 23 September 2023); Luiijf and others (n 2) 6.
25 Q Eijkman 'Indiscriminate bulk data interception and group privacy: Do human rights organisations retaliate through litigation?' in L Taylor and others (eds) *Group privacy: New challenges of data technologies* (2017) 162.
26 E Sutherland 'Digital privacy in Africa: Cybersecurity, data protection and surveillance' https://ssrn.com/abstract=3201310 (accessed 31 March 2023).
27 Y McDermott 'Conceptualising the right to data protection in an era of big data' (2017) *Big Data and Society* 4.
28 D Broeders and others 'Big data and security policies: Towards a framework for regulating the phases of analytics and use of big data' (2017) 33 *Computer Law and Security Review* 309, 319-320; ML Sundquist 'Online privacy protection: Protecting privacy, the social contract, and the rule of law in the virtual world' (2012) *Regent University Law Review* 153, 171.

unimaginable pathways for data collection and unobtrusive monitoring in cyberspace, for example, through digital 'cookies' or mobile phone applications, which allow unlimited access to personal information that may be easily misused or turned over to the government.[29] Concerning the proportionality of such data-gathering methods, international human rights institutions (dealt with in part 3 below) and civil society organisations have weighed in several times. The widely-acclaimed International Principles on the Application of Human Rights to Communications Surveillance of 2013 is one such intervention.[30] Relatedly, most modern democratic and hybrid legal regimes have aggregated several core general principles on privacy and cyber privacy, which are hereby re-iterated.

(1) Activities within homes enjoy the greatest level of protection from intrusion except on reasonable grounds and based on judicial orders.
(2) The privacy of activities within perimeters of the home may be protected at varying levels based on a 'reasonable expectation of privacy' or statutory provision.
(3) Activities carried out publicly may enjoy little or no privacy protection absent special statutory protection.
(4) Access to public services subject to data collection and regulated by the state may carry lesser or no privacy protections.
(5) Activity-related data may be processed if the data subject consents and if no prohibition exists for its processing.[31]

Moreover, the routine or indiscriminate processing of data would make it difficult to keep abreast of why and how data is being processed. That is why data protection rules are required to protect individuals against surveillance and foster accountability by public institutions. This is vital to protect citizens against the unconscionable exercise of government power in a democracy.[32]

Consequently, the framework of online privacy protection must focus on the asymmetric relations between individuals and the state to ensure that surveillance conducted for the public good must be demonstrably seen to achieve its purpose. This must be in a manner consistent with the cherished democratic values of autonomy, accountability and transparency. Indeed, Abdulrauf and Fombad, referring to De Hert and Gutwirth, traced the origin and development of data protection principles to the inadequacy of privacy *simpliciter* and as a mechanism to reconcile conflicting values of privacy and government surveillance in a democracy.[33] The respect for autonomy based on the informed consent of

29 Eijkman (n 25) 154.
30 Electronic Frontier Foundation 'Necessary and proportionate', http://www.necessaryandproportionate.net/ (accessed 23 September 2023).
31 Elmaghraby & Losavio (n 20) 493.
32 G de Gregorio 'Digital constitutionalism, privacy and data protection' in G de Gregorio *Digital constitutionalism in Europe*: *Reframing rights and powers in the algorithmic society* (2022) (ch 6) 216, 222-223; V Boehme-Neßler 'Privacy: A matter of democracy. Why democracy needs privacy and data protection' (2016) 6 *International Data Privacy Law* 222, 232; DJ Solove *Nothing to hide: The false trade-off between privacy and security* (2011) 93.
33 LA Abdulrauf & CM Fombad 'Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms' (2017) 38 *Liverpool Law Review* 105, 109-110.

individuals is a primary principle of digitised data protection that lends weight to a democratic theory of online privacy in the age of cyber insecurity. Consent, other basic principles of data privacy such as the so-called Fair Information Processing Principles (FIPP),[34] as well as other rules that enhance an individual's control over personal information comprise the norms of any data privacy system.[35] This means that individuals must have the right to control the way their data is collected, used and shared, which enlivens the right to be informed about data collection, the right to access and correct data, the right to delete data, and the right to withdraw consent to data processing. Online privacy should be protected by ensuring that individuals have reasonable control over their personal data so they can choose how it is collected, used, stored and shared. Security of data should be maintained by ensuring that it is protected from unauthorised access, use and disclosure. Moreover, data processors must be transparent and fair in their processing activities. This includes providing clear and accessible information on the data processing activities they conduct, the purposes for which they process data, the types of data they process, and how data is shared, if at all. Also, every democracy should provide measures to ensure that those responsible for collecting, storing and using data are held accountable for any misuse, unauthorised access or privacy breaches. This should include measures to ensure that data is processed in accordance with the principles on penalties for data breaches and a system of oversight and monitoring.[36] This means that there should be an external mechanism for ensuring that organisations are respecting individuals' online privacy rights and for the auditing of government surveillance programmes.

Considering the foregoing, international human rights institutions, intergovernmental bodies, privacy advocates and non-governmental organisations (NGOs) continue to grapple with how to ensure that the cybersecurity measures adopted by states do not stultify online privacy. This issue is extensively considered in part 3 below.

3 Online privacy and cybersecurity: International and African perspectives

The quest for cybersecurity has taken centre stage in global policy due to increased cyber criminality, including identity thefts, distributed denial of service (DDOS), internet hacking and even cyberterrorism, the prevention and prosecution of which may require states to access or collect personal data from

34 These include proportionality, minimality, purpose limitation, data subject influence, data quality, data security and sensitivity; see L Bygrave *Data privacy law: An international perspective* (2014) 145-165.

35 LA Abdulrauf 'Giving "teeth" to the African Union towards advancing compliance with data privacy norms' (2021) 30 *Information and Communications Technology Law* 87, 89-94.

36 See Organisation for Economic Cooperation and Development (OECD) Guidelines on the protection on privacy and transborder flows of personal data adopted 23 September 1980 para 11 (OECD Privacy Guidelines).

third parties, including business enterprises, or to intercept, disclose or share digital communications and intelligence data. This has made the protection of online privacy more challenging. Yet, efforts by the international community and regional institutions to address profiling, automated decision making, the gathering of sensitive personal information and resolve other challenges at the intersection of cybersecurity (as a sub-set of state security) and privacy have been faltering under the domain of cyber sovereignty.[37] The desired results are within reach if an international consensus on data control policy could be achieved.[38] This part engages with the evolving human right to digital privacy and its implications for personal data security within the ambience of state surveillance.

3.1 International human rights law and the cybersecurity-privacy conundrum

The international legal protection of online privacy, which lies at the heart of the networked information society, is a relatively recent concern, the normative basis of which derives from extant international human rights instruments negotiated under the auspices of the United Nations (UN), including article 12 of the Universal Declaration of Human Rights 1948 (Universal Declaration)[39] and article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR).[40] The right to online privacy protects personal data from misappropriation or unlawful use and is the enabler of the panoply of digital rights that are activated through the internet, smartphones, electronic communication media, search engines, social media networks, and computational technologies. This emergent right can be found in a patchwork of international soft laws. The interventionist elaborations by various human rights mechanisms, special procedures and other inter-governmental bodies acting under the auspices of the UN on 'the right to privacy in the digital age' confirm that this is a vital right.[41]

For instance, the 5 July 2012 resolution of the UN Human Rights Council (UNHRC) heralded the emergence of digital rights when it affirmed: '[T]he same rights that people have offline must also be protected online.'[42] These extend

37 EB Sultanov and others 'Transformation of the right to privacy in the context of the development of digital technologies' (2022) 7 *BiLD Law Journal* 223, 228.

38 ML Rustad & TH Koenig 'Towards a global data privacy standard' (2019) 71 *Florida Law Review* 365, 453.

39 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks' (UN 1948).

40 '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks' (UN 1966). See also regional instruments such as the European Convention on Human Rights (European Convetion) and the Inter-American Convention on Human Rights.

41 The UN Guidelines for the Regulation of Computerised Personal Data Files was the first attempt under the auspices of the UN that broached concrete protection for personal data.

42 'The promotion, protection and enjoyment of human rights on the internet' (A/HRC/RES/20/8). See also 'The promotion, protection and enjoyment of human rights on the

to privacy online,[43] which states are obligated to protect in the digital context by adopting legal, policy and other measures on data protection. In addition, technical solutions such as privacy-enhancing technologies (PETs) are required in the design of new technologies.[44] This is meant to give consumers more control over their online activities and prevent abuses through state surveillance or by businesses collecting, processing, sharing and storing biometric information in compliance with international human rights law. The UN through the General Assembly and the UNHRC also maintain that arbitrary surveillance and interception of communications, the arbitrary collection of personal data and the indiscriminate use of biometric technologies violate the right to privacy.[45] The UN has since 2013 in a General Assembly Resolution taken a stance against the tendency by states towards mass surveillance because of its implications on privacy. The Resolution called on states 'to respect and protect the right to privacy', especially in the context of electronic surveillance and digital communications.[46] Similarly, the 'United Nations Human Rights Report 2022' Office of the UN High Commissioner for Human Rights (OHCHR) 2022 Report amply demonstrates that general public surveillance is disproportionate and should be subject to judicial oversight.[47] Moreover, states are obliged to protect the 'confidentiality of [digital] communications'.[48] This may be done through encryption, pseudonymisation, anonymity and other measures, which means that anonymising technologies are vital for the uninhibited expression of views and exchange of ideas by individuals and groups online.[49] The UN General Assembly has also noted that 'privacy online is important for the realisation of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association'.[50] Considering the important of data privacy, the UNGA has called upon states:[51]

To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding

internet' (A/HRC/20/L.13), United Nations General Assembly Resolution, adopted by the Human Rights Council on 29 June 2012.

43 'The promotion, protection and enjoyment of human rights on the internet' (A/HRC/32/L.20), Resolution adopted by the Human Rights Council on 27 June 2016 para 8.

44 Para 5.

45 UN General Assembly Resolution 71/199 (2017); 'The right to privacy in the digital age' Human Rights Council Resolution 42/15 adopted at its 42nd session on 26 September 2019.

46 UNGA Resolution 68/167 on 'the right to privacy in the digital age', https://ccdcoe.org/sites/default/files/documents/UN-131218-RightToPrivacy.pdf (accessed 31 March 2023).

47 OHCHR Report 2022 412.

48 'The right to privacy in the digital age' (A/HRC/39/29) UNHCHR Report of 3 August 2018 para 20.

49 UNHCHR (n 48).

50 Resolution on the 'promotion, protection and enjoyment of human rights on the internet'.

51 'The right to privacy in the digital age' UNGA Resolution A/RES/68/167 adopted 18 December 2013, http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed 31 March 2023); 'The right to privacy in the digital age' UNGA Resolution A/RES/69/166 adopted 18 December 2014, https://undocs.org/en/A/RES/69/166 (accessed 31 March 2023).

the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law'.

However, while potentially legitimate circumstances may exist to protect national security, democratic states often ignore these guidelines to justify mass surveillance, bulk data and metadata collection concerning their citizens based on the cybersecurity narrative. As UNGA Resolution 68/167 recalls, any limitation by data surveillance to the right to privacy must satisfy a tripartite test of legality, legitimacy and democratic necessity. In a nutshell, a limitation must be provided in a clear and accessible law (as to its authorisation or circumstances) which provides for safeguards and oversight against abuse; serve a legitimate purpose (which includes state security); and be necessary towards such legitimate purpose (that is, state security). Ultimately, international human rights law will juxtapose compelling interests of cybersecurity with the values of online privacy to ensure that a limitation is proportionate in terms of a cost and benefit analysis (to the aim, be least intrusive, and rationally connected to the legitimate aim.[52] In addition, an assessment of proportionality requires transparency of the surveillance, its purpose and the likelihood of its objective being achieved.[53]

Relatedly, besides the well-known article 8 privacy protection in the European Convention on Human Rights and Fundamental Freedoms 1950 (European Convention), the EU is the global norm leader in data privacy in terms of its network of instruments and obligations of collection, use, safeguards, and so forth, placed on data controllers and processors.[54] In a nutshell, the foregoing correspond with the EU Charter of Fundamental Rights to the effect that data processing must be fair and lawful; for specified and lawful purpose(s); adequate and non-excessive in relation to purpose; accurate and up-to-date; and not kept for longer than is necessary; in accord with data subjects' rights (for example, non-transfer to a jurisdiction not having reciprocal adequate protection, and so forth).[55] Most significantly, an independent state institution, such as a data protection commissioner, must be statutorily mandated to monitor and enforce data protection rules. Such concerns have been brought closer home to African

52 UNODC 'International human rights and cybercrime law', https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-human-rights-and-cybercrime-law.html (accessed 23 September 2023).

53 Geneva Academy 'The right to privacy in the digital age: Meeting Report', https://www.geneva-academy.ch/joomlatoolsfiles/docmanfiles/ReportThe%20Right%20to%20Privacy%20in%20the%20Digita l%20Age.pdf (accessed 21 September 2023).

54 See OECD Privacy Guidelines (n 36) paras 7-14; E-privacy Directive; Council of Europe (CoE) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 108 of 1981 (CoE Convention 108/1981); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation) (principles on the processing of personal data) OJ 2016 L 119/1, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed 31 March 2023); Charter of Fundamental Rights of the European Union (OJ C 364 of 18 December 2000) art 7 (Charter), http://www.europarl.europa.eu/charter/pdf/text_en.pdf (accessed 31 March 2023); EU-US Safe Harbour Pact and its amendment; McDermott (n 27) 1-7.

55 See EU Charter of Fundamental Rights art 8(2).

governments and multilateral institutions on the need to reckon with canons that underline the protection afforded by privacy-related laws that have been recognised internationally.[56]

3.2 African data privacy regime

In Africa the increased internet access and penetration and ownership of smartphones have created a networked society with significant boosts for commerce and governance particularly in the telecoms industry,[57] although the data protection field remains fluid which has facilitated government surveillance. State surveillance, particularly, has grown in sophistication due to the increased availability of intrusive technologies to authoritarian governments to monitor citizens and political dissenters.[58] There is also increasing evidence of 'pervasive surveillance programmes and data mining activities' on the continent 'obviously in violation of data privacy norms'.[59] In Africa, just like in other climes, since the ultimate goal of surveillance is to collect information that, in most cases, relates to or identifies an individual, data protection laws have a direct bearing and are among the category of legal instruments that have been established specifically to regulate the gathering of personal information by electronic means including electronic surveillance.[60] Also, considering the improved access to internet technologies and related infrastructures, Africans are now becoming more concerned not only about the safety of critical ICT infrastructure from opportunistic cyber-attacks, but also the need to safeguard the fundamental rights of persons against the risks associated with the security of personal data shared online.[61]

Africa's first multilateral instrument to protect data privacy on the continent was the Supplementary Act A1SA.1f01f10 on Personal Data Protection Within Ecowas (EPDP Act). It was signed by member states of the Economic Community of West African States (ECOWAS) on 16 February 2010 in Abuja, Nigeria. The EPDP Act, to some extent, is patterned after the former EU 'Directive 95/46/EC', that is, Data Protection Directive with the objective of 'a harmonised legal framework in the process of personal data' within ECOWAS member states.[62] The EPDP Act protects the data of an identifiable individual through eight principles

56 J Terstegge 'Privacy in the law' in M Petkovíc & W Jonker (eds) *Security, privacy, and trust in modern data management* (2017) 13-14; OECD Privacy Guidelines (n 36) para 1(b); CoE Convention 108/1981.
57 Sutherland (n 27).
58 As above.
59 Abdulrauf (n 36) 88.
60 LA Abdulrauf 'The challenges for the rule of law posed by the increasing use of electronic surveillance in sub-Saharan Africa' (2018) 18 *African Human Rights Law Journal* 365, 372-374.
61 R Alunge 'Africa's multilateral legal framework on personal data security: What prospects for the digital environment?' (2020) 38-58, https://doi.org/10.1007/978-3-030-41593-8_4 (accessed 30 March 2023).
62 EPDP Act, Preamble.

of data processing, the foremost being the consent of data subjects.[63] Others are fairness, specification of purpose, accuracy, transparency, confidentiality, and so forth.[64] The latter requires the protection and confidentiality of personal data, particularly during transmission over a network.[65] The EPDP Act mandates the establishment of an independent data protection authority with powers to protect the data-related rights of persons, to hear complaints, issue compliance directives, and penalise any controller or processor of data for the contravention of relevant rules.[66] The EPDP Act is directly binding on Nigeria as a state party by virtue of the revised ECOWAS Treaty of 1975. The EPDP Act was followed by the AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention), adopted in Malabo on 27 June 2014.

The African Commission on Human and Peoples' Rights (African Commission) – the AU continental body mandated to promote human and peoples' rights – has elaborated on the right to privacy in the digital age. The African Commission's Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019' (DoP 2019) reads:[67]

> (1) Everyone has the right to privacy, including the confidentiality of their communications and the protection of their personal information.
> (2) Everyone has the right to communicate anonymously or use pseudonyms on the internet and to secure the confidentiality of their communications and personal information from access by third parties through the aid of digital technologies.

Furthermore, DoP 2019, which is legally non-binding, obligates states to provide safeguards for the right to privacy in terms of 'any law authorising targeted communication surveillance' such as through 'the prior authorisation of an independent … judicial authority', 'specific limitation on the … scope of the surveillance' and other 'due process safeguards'.[68] The 'notification of the decision authorising surveillance within a reasonable time' post-conclusion, transparency thereof, and regular 'monitoring and review by an independent oversight mechanism' are other germane requirements.[69] However, the EU Data Protection Directive 1995, the *General Data Protection Regulation* (GDPR)'s forerunner's influence in the drafting of data protection laws in Africa, cannot be underrated more, with the result that the African Charter on Human and Peoples' Rights of 1981 (African Charter), the flagship African human rights treaty, has no

63 EPDP Act art 23.
64 EPDP Act arts 24-29.
65 EPDP Act art 28.
66 One Trust Data Guidance 'African bodies: ECOWAS Act on Personal Data Protection', https://www.dataguidance.com/opinion/african-bodies-ecowas-act-personal-data-protection (accessed 31 March 2023).
67 Adopted by the African Commission at its 65th ordinary session held from 21 October to 10 November 2019 in Banjul, The Gambia, Principle 40.
68 DoP 2019 Principle 41(2)(3)(a)(b)(c).
69 DoP 2019 Principle 41(3)(d)(e)(f).

privacy provision.[70] While most African states have privacy protection in their constitutions, the right to online privacy is embryonic and suffers from poor implementation in the face of data retention conditions imposed on digital intermediaries and social network platforms by authoritarian governments.[71]

Nonetheless, the AU Convention on Cyber Security and Data Protection 2014 draws inspiration from CoE's Convention 108/1981 to provide a template for cybersecurity and protection of personal information in Africa.[72] The Convention is a great boost for data protection and privacy in Africa and provides a laudable standard for the right to online privacy that can be adapted by Nigeria and other African countries. The Convention became operative on 8 June 2023 after Mauritania deposited its instrument of assent with the AU Chairperson being the fifteenth AU state to do so in terms of its provisions.[73]

3.2.1 Data privacy and protection in Africa: An overview

In bridging the normative gap on data privacy and protection on the continent, the ministers on information technology (IT) in Africa secured the AU Commission (AUC) and UN's regional Economic Commission for Africa's assistance in preparing a Declaration on Cybersecurity for the African context based on the principles of data protection and cybersecurity. The Declaration was eventually adopted by African Heads of State and Government at its meeting held in Malabo in 2014 as the AU Convention on Cyber Security and Data Protection 2014 (Malabo Convention), an analysis of which hereby follows.

The Convention provides for the establishment of a National Personal Data Protection Authority as the supervisory and regulatory body and the *loci* of enforcement with authority, among others, to prescribe sanctions for violations.[74] The Malabo Convention prescribes six basic principles of data processing towards individual data privacy. First, the data subject's consent must be obtained before their data is processed. Confidentiality and security are required particularly when personal data is transmitted over a computer network. Second, data processing must be fair and lawful. Third, the processing of data must serve a specific or related purpose (purpose limitation). Fourth, data controllers must ensure that data is up-to-date and erase or amend it when inaccurate or incomplete (data

70 The African Charter on the Rights and Welfare of the Child protects the right to privacy; see AB Makulilo 'Privacy and data protection in Africa: A state of the art' (2012) 2 *International Data Privacy Law* 163, 168-171.

71 YE Ayalew 'The right to privacy in the digital era in Africa' (2022) 12 *International Data Privacy Law* 16, 19.

72 Signatory countries to the ECOWAS Treaty including Nigeria have undertaken obligations under the EPDP Act to create legislative, policy and other actions as regards 'personal data protection' subject to public interest.

73 African Union 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection', https://dataprotection.africa/wp-content/uploads/2305121.pdf (accessed 10 September 2023).

74 AU Cybersecurity Convention arts 11, 12(2) & 19(1)(f).

accuracy principle). Fifth, data controllers must process data in a transparent manner (transparency principle). Lastly, the principle of confidentiality obligates data controllers to process personal data in secure and confidential ways.[75] In addition, specific principles apply to the processing of sensitive personal data. these include data that relate to intimate relationships, sexual orientation, religious inclination, political persuasion, and so forth.[76] Furthermore, as regards the rights of data subjects, the Convention provides for the right to information, to access data, the right to object to data processing, and to rectify data.[77] These embody the entitlements of the individual to demand from a data controller the extent to which her data has been processed, shared or disclosed to a third party. The coverage of data privacy under the Convention, therefore, extends to photographs, voice messages, emails, internet login passwords, search history, and so forth.

The 'principle of confidentiality and security' must be operationalised any time personal data is to be transmitted over a (computer) network. Data controllers under both the Convention and ECOWAS Data Act will perform the same duties as regards data security.[78] Moreover, a data controller must be ready to give the assurance of data security and will be vicariously liable for any breach thereof even when an independent data processor works for it.[79] The Convention makes the DPA the *loci* of enforcement, monitoring and supervisory activities being entitled to '[e]ntertaining [of] claims, petitions and complaints regarding the processing of personal data' and violations of data security but must advise petitioners on the way forward.[80] As regards data subjects' rights, there is a right to access and rectify data.[81] These embody the data subject's entitlements to demand to know the extent to which their data has been processed, shared or disclosed to a third party. In addition, other Convention rights as regards personal data protection include access to information, data access, objection to data processing, and 'to be forgotten'. The coverage of data privacy under the Convention, therefore, extends to photographs, voice messages, emails, internet login passwords, search history, and so forth, which should, however, not detract from the need for free flow of data. The 'processing of personal data relating to public security, defence, research, criminal investigation or state security' can also be undertaken, but subject to the provisions of other existing laws.[82]

Notably, the Convention aims to commit parties thereof to cybersecurity policy and strategy and legal instruments to respond to cyber-attacks and cyber-crimes that adequately satisfy the security interests of the state and protect online

75 AU Cybersecurity Convention arts 13(1)-(6).
76 AU Cybersecurity Convention art 14.
77 AU Cybersecurity Convention arts 16, 17, 18 & 19; EPDP Act arts 38(6) & 39.
78 AU Cybersecurity Convention arts 20 & 21.
79 AU Cybersecurity Convention art 13(b); EPDP Act art 29.
80 AU Cybersecurity Convention art 12(2)(e); EPDP Act art 19(1)(f).
81 AU Cybersecurity Convention art 17; EPDP Act arts 38(6) & 39.
82 AU Cybersecurity Convention art 9(1)(d).

privacy in consonance with personal data protection.[83] The Convention applies to personal data processing, automated or otherwise, by individuals and public institutions in a state party's territory.[84] However, it is subject to exemptions or authorisations by a state for the processing of data for 'state security', 'defence', and 'sensitive data' and in terms of 'an executive or legislative act'.[85] So, considering that the AU Cybersecurity Convention is a model law, how it is implemented by its state parties will determine the extent to which the state and private businesses will be able to process data, intercept calls, and carry out surveillance without subject to the requisite safeguards and oversight.

Now, given the foregoing targeted international and African human rights-focused analyses, the next activity of this article is to engage with Nigeria's privacy and cybersecurity landscape.

4 Nigeria's constitutional and legal safeguards for online privacy

This part engages with an analysis of the cybersecurity and surveillance laws, policies and practices in Nigeria and assesses their compatibility with the right to online privacy, starting with an overview of Nigeria's constitutional framework on the domestic application of international human rights. The analysis exposes the potential risks and harms associated with state surveillance and inadequate cybersecurity measures on online privacy in Nigeria.

Under the amended Constitution of the Federal Republic of Nigeria, 1999 (1999 Constitution, CFRN 1999 or Constitution) an international treaty or agreement must be incorporated into the domestic legal framework before it can bind institutions, persons and the government.[86] This is the case with the African Charter. Even where not yet incorporated into domestic law, a treaty signed or ratified by the country is binding based on the principle of *pact sunt servanda* whereby the government may not act contrary to its undertaking. The provisions of an unincorporated treaty may also be relied upon by the courts as an interpretive aid in construing other legal instruments not contrary thereto. The human rights provisions in chapter IV of the Constitution also borrowed extensively from the Universal Declaration and have also ratified several other human rights treaties that guarantee human rights, including the right to privacy under ICCPR. This makes the tripartite tests of legality, necessity and legitimacy applicable to the limitations of such rights. Moreover, Nigeria developed a National Security Policy and Strategy in 2014 (updated in 2021) and passed

83 AU Cybersecurity Convention Preamble, arts 1 & 8(1).
84 AU Cybersecurity Convention Preamble, arts 24 & 25(3).
85 AU Cybersecurity Convention arts 5(a)(d), 9(1)(a)-(d) & 10(4)(a)-(d).
86 CFRN 1999 sec 12.

the Cybercrimes Act 2015 and Data Protection Act 2023 partly in terms of its obligations under the AU Cybersecurity Convention.

4.1 Privacy and the emergence of digital communications

CFRN 1999 recognises privacy as an inalienable human right, but the need for robust laws and policies to protect the citizens' digital rights, including online privacy, only sparsely receives attention from policy makers considering the extant patchwork of legislations and regulations.[87] Section 37 of CFRN 1999 reads: 'The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected.' The provision guarantees the right to privacy of family life, homes, correspondences, telephone and telegraphic communications of Nigerians from unlawful interference by the state and non-state agents. Section 37 mimics an earlier provision that was first drafted in the era of analogue telephones (fixed landlines), telegraphic and telex services when internet-enabled devices and computer networks were still a rarity in Nigeria.[88] In addition, the common law of torts applicable in Nigeria does not recognise a general tort of privacy, although a limited common law action for breach of confidence could be relied upon to remedy a wrongful interference with personal data. Even such a limited legal right remains subject to restrictions under some inherited colonial/military era statutes such as the Official Secrets Act 1962 (OS Act 1962)[89] and National Security Agencies Act 1986 (NSA Act 1986)[90] that deny public access to state secrets and sensitive law enforcement, foreign relations and national security-related information.

The opening-up of political space in the aftermath of the democratic transition in 1999 led to improvements in individual and collective freedom of digital communications in Nigeria. Consequently, the Nigerian Communications Act 2003 (NC Act),[91] the main legal and regulatory framework on electronic and digital communications, was enacted and established the Nigerian Communications Commission (NCC) as the regulatory body for Nigeria's telecoms industry. The NC Act 2003 obligates licensees or service providers to

87 Reference could be made to the following: Central Bank of Nigeria; Consumer Protection Framework 2016 (bank customers' right to confidentiality); Credit Reporting Act 2017 (protects data subjects' right to privacy and confidentiality of their credit); Child Rights Act 2003 (guarantees the child's right to privacy of correspondence, telephone communications, etc, subject to parental or legal guardians' reasonable supervision): National Health Act 2014 (makes information relating to a healthcare user confidential, sets out conditions for the disclosure of such information, and prescribes measures to safeguard health records); Consumer Code of Practice Regulations 2007 issued by the Nigerian Communications Commission (requires telecommunication operators to take reasonable steps to prevent 'improper or accidental disclosure of data and ensure safe storage of personal information; Freedom of Information Act 2011 (requires the government to protect personal privacy by denying access to personal information unless the individual concerned consents.

88 Constitution of the Federal Republic of Nigeria 1979 (as amended) sec 37.

89 Cap O3 Laws of the Federation of Nigeria (LFN) 2004.

90 Cap N7 LFN 2004.

91 Act 19 of 2003.

'upon written request by the Commission or any other authority, to assist as far as reasonably necessary' in preventing an offence, enforcing the law, and in the preservation of national security.[92] Section 146(3) of the NC Act protects licensees from any liability while carrying out any such duty. The NCC may also determine that a licensee or class of licensees implement the capability to allow authorised interception of communications.[93] This could be in the event of a public emergency, in the interest of public safety, to protect national security, and so forth.[94] Pursuant to its enabling powers, the NCC has made some regulations and codes relating to the protection of subscribers' personal information.[95] This article tracks only those directly related to state surveillance.

The Lawful Interception of Communications Regulations 2019 (LICR 2019), pursuant to the NC Act 2003, set out the conditions in which communications originating from Nigeria may be intercepted, collected and disclosed. The LICR 2019 permits an 'authorised agency' such as the State Security Service (SSS) and the Office of the National Security Adviser (NSA) to intercept any communication in Nigeria based on a court warrant. Warrantless interception and monitoring of online communications are authorised to prevent danger to human life or where otherwise necessary, although judicial authorisation must be obtained within 48 hours thereof. The authorised agencies must submit an annual report of all concluded interception cases to the Attorney General of the Federation (AGF). This creates a real conflict of interest situation considering that the AGF is expected to publicly scrutinise the secret activities of a government from which she benefits politically.

Relatedly, the Registration of Telephone Subscribers Regulations 2011 (RTSR 2011) mandates licensees to capture subscriber information and to transmit such to a central database to be established and maintained by the NCC. The latter can grant security agencies access to the database provided it receives a prior written request from an official, not below the rank of an Assistant Commissioner of Police (ACP) or coordinate rank. Furthermore, RTSR 2011 mandates licensees to retain call data, which may also be released by the NCC upon a written request to it signed by a police officer at or above the rank of ACP or equivalent.[96] All the foregoing provisions call for a law targeted at data privacy, the safeguarding of computer networks from criminal interference and the continuous promotion of technological innovation.

92 NC Act 2003 sec 146(2).
93 NC Act 2003 sec 147.
94 NC Act 2003 sec 148(1).
95 See, eg, the Federal Republic of Nigeria Official Gazette, Nigerian Communications (Enforcement Process, etc) Regulations 2019, https://www.ncc.gov.ng/docman-main/legal-regulatory/regulations/840-enforcement-processes-regulations-1/file (accessed 30 March 2023); Consumer Code of Practice Regulations 2007 (CCPR 2007) and its Schedule, the General Consumer Code of Practice (GCCP).
96 RTSR 2011 Reg 8 (2)(a)(b).

4.1.1 Cyber-crimes and data privacy

Globalisation and e-commerce, aided by the internet, technological developments and improvement in IT infrastructure and digital technologies, have percolated down to Nigeria, but the authorities were late in responding to the cybersecurity threats and criminality related thereto until very recently. Several policy initiatives of the government have now been enunciated. There is the National Cybersecurity Policy and Strategy 2021 (NCPS 2021) adumbrated by the National Security Adviser (NSA),[97] which focuses on safeguarding Nigeria's critical infrastructure and the protection of its cyber-space from cyber-attacks, online fraud, and so forth, besides its economic outlook.[98] The National Digital Economy Policy and Strategy 2020-2030 from Professor Isa Pantami-led Digital Economy Ministry also addresses the nation's cybersecurity challenges to enhance the national digital economy.[99] Based on these policy responses, state surveillance has increased and is becoming more widespread even with the enactment of cyber-crime laws. This has negative impacts on online privacy rights and other fundamental freedoms. For example, Nigeria's Cybercrimes (Prohibition, Prevention, etc) Act, 2015, which was enacted to strengthen the fight against organised crime, criminalises unauthorised access to computer systems.[100] The law also criminalised certain activities carried out in cyber-space with a computer or through computer systems and networks. These include cyber-stalking, sending obscene, menacing or hate messages, internet fraud, cyber-terrorism, and so forth.[101] Incidentally, some of these offences have been targeted at journalists, bloggers and the political opposition while their phrasing is open-ended, thus giving a cause for concern.[102] Section 38 of the Cybercrimes Act also permits data and traffic retention by internet intermediaries and telecom companies for two years at the government's request. Notably, the retained data 'shall not be utilised except for legitimate purposes as may be provided for under th[e] Act, any other legislation', whilst the authority to use such information must be exercised with 'due regard to the individual's right to privacy' while 'tak[ing] appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved'.[103] However, what

97 Federal Republic of Nigeria 'National cybersecurity policy and strategy 2021', https://ctc.gov.ng/national-cybersecurity-policy-and-strategy/ (accessed 22 September 2023).

98 N Okoh '2021 national cybersecurity policy and strategy: Enhancing digital safety and economic growth' *The Journal* 25 February 2021, https://thejournalnigeria.com/cybersecurity-policy-strategy-digital-safety-economic-growth/ (accessed 30 March 2023).

99 Federal Ministry of Communications and Digital Economy 'National Digital Economy Policy and Strategy 2020-2030', https://www.ncc.gov.ng/docman-main/industry-statistics/policies-reports/883-national-digital-economy-policy-and-strategy/file (accessed 23 September 2023).

100 Cybercrimes Act 2015 sec 6.

101 Cybercrimes Act 2015 secs 24(1)(a) & (b).

102 In *The Incorporated Trustees of Rights and Laws Awareness v Nigeria* Suit ECW/CCJ/APP/53/2018 (judgment delivered on 10 July 2020), the ECOWAS Court of Justice struck down section 24 of the Cybercrimes Act that prescribes the offence of cyberstalking for vagueness; see Sahara Reporters 'ECOWAS Court declares Nigeria's Cybercrime Act section 24 vague, arbitrary, unlawful', https://saharareporters.com/2023/03/22/ecowas-court-declares-nigerias-cybercrime-act-section-24-vague-arbitrary-unlawful (accessed 30 March 2023).

103 Cybercrimes Act 2015 sec 38(4)(5).

amounts to 'legitimate purposes' is not specified while there is no provision on the notification of data breach under the Act.

4.1.2 The Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023 (NDP Act 2023, NDP Act or Act) was enacted in reforming the overall legal framework for data protection. It replaces the erstwhile Nigeria Data Protection Regulations 2019 (NDPR 2019) issued by the National Information Technology Development Agency (NITDA).[104] The Act is applicable only where the processing of personal data occurs within the Nigerian jurisdiction concerning a data subject within Nigeria or by a data controller or processor who markets to or monitors residents within Nigeria. The Act establishes the Nigeria Data Protection Commission (NDPC) with a governing council to be headed respectively by political appointees, which creates the issue of independence from the government. The Act mimics the EU's GDPR in several respects. For instance, it defines personal data as 'any information relating to an identified or identifiable natural person' or individual, that is, the data subject. This includes personal data and metadata such as a name, address, photo, email address, bank details, social media posts, medical information, or a computer's IP address. The NDP Act enunciates six principles of data processing: (i) fair, lawful and transparent processing, that is, with the consent of the data subject and for the performance of the data subjects' legal obligation, vital interests or the public interest; (ii) purpose specification, that is, only for specified, explicit and legitimate purposes and no further processing in an incompatible manner; (iii) adequacy, that is, limited to the minimum necessary for collection or further processing; (iv) limited retention, that is, not retained for longer than necessary; (v) accuracy, that is, complete and kept up-to-date; (vi) data security, that is, processed in a manner that secures against loss, destruction, or any form of data breach.[105] Several safeguards against unlawful processing include a data protection impact assessment (DPIA)[106] and improvement in the rules on the processing of sensitive personal data.[107]

It is worth noting that the Act has created substantive data protection and privacy standards against which the plethora of regulations and policies regarding the creation of databases in Nigeria must be subsumed. For instance, the e-communications regulatory environment currently is riddled with requirements for biometrics registration and the creation of e-databases as part of the ongoing modernisation of e-governance processes in the banking, health, educational and

104 Aelex 'A summary of the Nigeria data protection Bill 2022', https://www.aelex.com/a-summary-of-thenigeriadata-protection-bill-2022/ (accessed 31 March 2023).
105 NDP Act 2023 sec 24.
106 NDP Act 2023 sec 28.
107 NDP Act 2023 sec 30.

other sectors in Nigeria.[108] Furthermore, the government through the NCC may direct telecom providers to collect, intercept or retain personal data for national security reasons without the requisite data subject's consent.[109] Such surveillance and data interception actions require serious scrutiny in relation to the NDP Act to assess their legality, legitimacy, democratic necessity and ultimate proportionality when carried out in the name of cybersecurity or national security.

4.2 Whither state surveillance?

Section 3(2) of the NDP Act 2023 exempts from its purview, subject to the human rights provisions of the Constitution and their limitations, the processing of personal data carried out by a 'competent authority' as is necessary for national security. Under section 3(3) the NDPC may by regulation prescribe the types of personal data and processing that may be exempted from application of the Act, while section 3(4) further empowers NDPC to issue a guidance notice as to legal safeguards and best practices as regards any aspect of data processing that is exempted if it violates or is likely to violate section 24 of the Act (the principles of data processing). Such 'competent authorities' are yet to be designated but they would ordinarily include the national security agencies established under the NSA Act 1986.[110] These are the Defence Intelligence Agency (DIA), the National Intelligence Agency (NIA) and the State Security Service (SSS) (otherwise called the DSS). Again, while the exemptions that have been envisaged under sections 3(2) and 3(3) are yet to be carved out, it is not inconceivable that the 'competent authorities' may rely on the NC Act, LICR 2019, NCPS 2021 and Cybercrimes 2015 as basis for the interception of communications (see also paragraphs 4.1 and 4.1.1 above).

State surveillance in Nigeria could easily fail the requirement of legality prescribed under international human rights law (part 3.1 above) because the judicial and political safeguards against abuse are not well-established. As already stated, Regulation 8(2) of RTSR 2011 empowers the NCC to demand the release of subscribers' data by service providers to the security agencies, while section 38 of the Cybercrimes Act 2015 permits the interception of communications but has not specified the legitimate national security purpose for such or the need to notify the data subject thereafter.[111] Regulation 18 of LICR 2019 permits

108 See the Federal Republic of Nigeria Official Gazette, Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011 (popularly called 'SIM card registration'), https://www.ncc.gov.ng/docman-main/legalregulatory/regulations/201-regulations-on-the-registration-of-telecoms-subscribers/file (accessed 31 March 2023); Bank Verification Number (BVN) registration; Electoral Act 2022 (mandatory registration for the e-voting system). Government has plans to merge these databases electronically for administrative purposes though many of these projects have turned up with incomplete or mismatched information while persons affected face serious hurdles to make corrections. See the National Identity Management Commission Act 2007 (NIMC Act 2007).

109 NC Act 2003 secs 146(2) & 147.

110 NSA Act 1986 sec 1(1)(a)(b)(c).

111 See RTSR 2011 Reg 8(2)(a)(b).

the intercepted communication to be stored for three years. The challenge relates to the security of such data. The legal provisions are also widely drafted, which is a 'red flag' for potential abuse. The legitimacy and democratic necessity of any so-called national security or defence rationale to intercept and analyse communications data, therefore, can be seriously queried.

Furthermore, there is a very troubling conflict between the two statutes governing the national security agencies and other statutes such as the NDP Act 2023. Under the NSA Act 1986, the *modus operandi*, spending and personnel matters of the national security agencies are state secrets that are not amenable to public or legislative scrutiny while it specifically voids other laws inconsistent with it.[112] Currently, there is no system of oversight for the national security agencies under the NSA Act 1986 while the one envisaged under NDP Act 2023 is not yet in place. Even the so-called oversight by the AGF under LICR 2019 is weak and questionable considering that the AGF might be politically defensive towards its political benefactors.

However, a brief comparative overview of the legal frameworks for national security and intelligence in South Africa and the United Kingdom can yield some insights into how these democratic countries provide for their oversight and audit which may be tapped and adapted for Nigeria. In South Africa, state surveillance by its State Security Service (SSA) and other agencies is permitted under the National Strategic Intelligence Act of 1994, Intelligence Services Oversight Act of 1994, Intelligence Services Act of 2002, and [General Intelligence Law Amendment Act] GILAA of 2013.[113] The latter statute expressly defines the term 'national security'. South Africa's Intelligence Services Oversight Act of 1994 created the parliamentary Joint Standing Committee on Intelligence (JSCI) and the Inspector-General for Intelligence, either of which may hear complaints of unlawful surveillance from citizens.[114] The JSCI, which is composed of members of different political parties, has the responsibility to scrutinise and report on the operations of the SSA. In the United Kingdom, the political oversight of the investigatory powers of the secret service, namely, the Secret Intelligence Service (MI6), Security Service (MI5), and Government Communications Headquarters (GCHQ), is handled by a parliamentary Intelligence and Security Committee (ISC) under Investigatory Powers Act of 2016 (IP Act 2016). Under the IP Act 2016, an ISC report concerning its work must be published every year.[115] To provide transparency and accountability, the IP Act 2016 also established the Investigatory Powers Commissioner's Office (IPCO) to oversee the use of GCHQ's operational powers and the Investigatory Powers Tribunal (IPT), an

112 NSA Act 1986 secs 3 & 7(2).
113 See E Sutherland 'Governance of cybersecurity – The case of South Africa' (2017) 20 *African Journal of Information and Communication* 96.
114 Sutherland (n 113) 96-97.
115 Investigatory Powers Act 2016 (UK) sec 234.

independent judicial body to grant redress to victims of unlawful investigation.[116] The IP Act 2016 provides that interception warrants will only be granted when authorised by a secretary of state and approved by a judicial commissioner and if proportionate to what it seeks to achieve, such as the interests of national security.[117]

4.3 Call for synergy of law and policy

Many democracies are adopting cybersecurity strategies encompassing laws, policies and practices to prevent crime and in sync with human rights law of data privacy, but several gaps in Nigeria's existing cybersecurity legal and policy frameworks in comparison to evolving international standards call for a synergy of law and policy. There is no gainsaying that the numerous public projects and methods through which personal data is obtained, processed and managed neglect the right to access by data subjects for needful correction. Purportedly acting for the national cybersecurity or economic interest, public and private agencies could hand over personal and communications data collected to security agencies without transparency, properly laid down procedures or later notification. This constitutes a violation of the right to online privacy and raises data protection concerns under the prevailing data protection regulations in Nigeria. Consequently, the strategies for the synergy of law and policy at the intersection of cybersecurity and online privacy should ordinarily encompass (i) a legislative oversight of national security agencies; (ii) collaboration between government and citizens to address cybersecurity threats and protect citizens' privacy; (iii) proposals for new laws and policies or the amendment of the ones existing to address the gaps in Nigeria's cybersecurity and online privacy laws such as the absence of a clear definition of 'national security'; (iv) the importance of public education and awareness to promote better cybersecurity practices; and (v) technological solutions and policy strategies such as privacy-enhancing technologies, and to strengthen the capacities and skills of data controllers and processors to adopt state-of-the-art technologies to ensure privacy by design and default.

5 Conclusion

The article has dwelled on the national appropriation of the advantages of internet penetration and ICT usage among Nigerians for commerce, socialisation and access to public services as a rapidly-advancing process. The vital gains of a digital economy and the global internet infrastructure are now being threatened by cyber-related crimes and other vices. It accords with democratic principles for

116 GCHQ Governance 'Oversight', https://www.gchq.gov.uk/section/governance/oversight (accessed 20 September 2023).
117 GCHQ Governance 'Legal framework', https://www.gchq.gov.uk/section/governance/legal-framework (accessed 21 September 2023).

the strategies and laws designed to arrest cyber criminality to be proportionately balanced by a data privacy law that meets international standards, but the situation in Nigeria currently is skewed in favour of the state despite the existence of the NDP Act 2023. This has grave implications for the enjoyment of online privacy and related freedoms by citizens, professional journalists and more politically-conscious persons. The situation also has broader implications for the protection of online privacy and cybersecurity in other contexts. Cybersecurity law and policy measures are needful but pose risks of overreaching the state's surveillance powers and consequent loss of control over personal data, including citizens' ability to communicate anonymously. Ensuring online privacy requires that state surveillance practices be transparent and limited and involves a call to action for policy makers, civil society organisations and other stakeholders in Nigeria to work towards compliance with the NDP Act 2023.

In addition to paragraph 4.3(i)-(v) above, the article recommends a synergistic approach to the enhancement of cybersecurity and privacy in Nigeria as being complementary in the internet age. Cybersecurity strategies and surveillance practices must be reformed through the injection of institutional safeguards and independent multi-party oversight as in the UK, increased public awareness and enhanced democratic participation. Since Nigeria now has a Data Protection Commission under the NDP Act 2023, it must establish its regulatory independence from the onset by swiftly imposing sanctions on errant data controllers and processors and enriching a safe online environment by creating awareness of the data subjects' rights. There is also the need to encourage private sector participation in cyber protection.

African Journal on Privacy & Data Protection

To cite: CA Khamala 'Digital surveillance and big data: Balancing the rights to privacy and security in Kenya' (2024) 1
African Journal on Privacy & Data Protection 176-206
https://doi.org/10.29053/ajpdp.v1i1.0009

Digital surveillance and big data: Balancing the rights to privacy and security in Kenya

*Charles A Khamala**
Senior Lecturer, Africa Nazarene University Law School; Academic Leader, Criminal Justice and Security Management

Abstract:

Education, personal identity and democracy flourish in private. Generalised surveillance of disenchanted groups stifles them. Although the African Charter on Human and Peoples' Rights is silent on the right to privacy, Kenya's Constitution expressly protects against surveillance abuse. Informed consent is required from data subjects prior to collecting or sharing their personal information. Yet, Kenyan courts have upheld laws and policies introducing generalised surveillance. The conundrum confronting Kenya's judiciary regarding surveillance of mobile telephone data is: If counter-terrorism relies on mass surveillance, such policies necessarily violate privacy rights, in the guise of enhancing security. Nonetheless, enhancing the state's surveillance capacity to intercept digital communications was accepted by the Court as a justifiable violation of privacy rights. Conversely, in *Communication Authority of Kenya v Okiya Omtatah Okoiti*, the Court of Appeal observed that globally, the theft of mobile phones and proliferating counterfeit devices have become major regulatory concerns. Problematically, it

* PhD in Droit Privé (Sciences Criminelles) Université de Pau et des Pays de l'Adour (France); LLM (London) LLB (Nairobi); PGDip KSL; [email] chalekha@yahoo.co.uk; ckhamala@anu.ac.ke.

reversed the High Court's prohibition on generalised surveillance. Subsequently, in *Katiba Institute v Attorney General*, the High Court directed the state to conduct a data protection impact assessment as the Data Protection Act requires. In April 2023, the Supreme Court dismissed the Law Society of Kenya's appeal seeking to stop the CAK embarking on a device management system, which threatens to surveil subscribers. Three conclusions emerge. First, Kenya's DPA accords absolute governmental power to gather personal data unrelated to national security or suspicion of crime. Second, the Court of Appeal's *Mobile Telephones* determination is oblivious to the chilling effect that any generalised surveillance creates even on groups that value confidentiality. Third, neither the National Intelligence Services Act nor the Prevention of Terrorism Act protect citizens' communications from limited interception. It is preferable to introduce similar provisions authorising interception of specific communications in other legislations to facilitate investigation of serious organised crimes.

Key words: chilling effect; data protection; group privacy; human dignity; informed consent; intercept communications; secret intelligence

1 Introduction

Traditional English common law knew no right to privacy. This was held in *Wainwright v Home Office*[1] where, despite being strip-searched with excessive force by prison officers, a visiting mother and son had no cause of action for a privacy violation. Privacy rights were first recognised in the late twentieth century law of torts. Nonetheless, individuals who make such claims must not only identify their tortfeasor. They must also specify the remedies sought. Yet, simply hacking someone's correspondence without disclosing its information to a third party makes the concrete harm difficult to substantiate. This is because the law does not concern itself with trivialities.[2] Worse still, big data's harmful potential may remain unknown at the point of gathering. Significantly, digital data is collected over long durations from numerous nondescript persons, without a pre-established purpose.[3] Only upon subsequent analysis by computer algorithms does it produce statistical correlations with informative value. The results invariably reveal behaviour patterns of individuals or groups in websites frequented by internet users or cryptic codes contained in emails or other electronic messages. Emergent information may give governmental authorities reason to suspect an individual of engaging in terrorist activities or violating other laws. Although liberal democratic constitutions empower governments to produce public goods, state power is limited by individual rights. Yet, because

1 [2003] QB 195, 205-6; [2004] 2 AC 406.
2 B van der Sloot 'Is the human rights framework still fit for the big data era? A discussion of the ECtHR's case law on privacy violations arising from surveillance activities' in S Gutwirth, R Leenes & P de Hert (eds) *Data protection on the move current developments in ICT and privacy/data protection* (2016) 415.
3 Van der Sloot (n 2) 413.

warrantless mass surveillance technology is inherently invasive, it violates the personal sphere. Therefore, to safeguard privacy rights, data protection legislation has proliferated worldwide. These laws purport to protect data controllers, comprising persons who gather and control information, against privacy breach lawsuits. In pertinent part, section 30(1) of Kenya's Data Protection Act (DPA) precludes data controllers or processors from processing personal data, unless such processing is necessary to protect the data subject or other individual's vital interests; or to perform a public interest task or in the exercise of the controller's vested official authority; or to perform any task by a public authority.[4] To the extent that this provision permits mass surveillance, it may therefore overreach section 3's intended purpose of protecting the privacy of individuals as read with section 25's data protection principles. This anomaly is attributable to big data's abstract nature. Consequently, individuals may be unaware of their personal data's excavation and disclosure to third parties, whether by fellow citizens using smart phones, or by companies' tracking cookies or even by the government using covert surveillance.[5]

The essential problem with all surveillance is that while potential harms are comparatively manifest, its benefits are inconspicuous. Many terrorist operations that covert intelligence helps foil, remain unknown to citizens. Moreover, the act of looking for terrorists, as Donoghue observes, 'may well involve obtaining information about a large number of people'.[6] Thus, surveillance operations delve deep into the state's social and political life.[7] Van der Sloot concludes that difficulties arising from mass surveillance operations and big data analytics by states cannot be characterised as human rights violations, but instead should be understood as demands for enhanced governance and a fair hearing, underpinned by legality and legitimacy principles.[8] The purpose of this article, therefore, is to construct a normative framework to examine big data's impact on privacy rights. The objective is to evaluate the constraints of mass surveillance through big data in the Kenyan context. This issue confronts Kenya's judiciary with numerous challenges by citizens against executive overreach regarding surveillance by big data. For example, in 2020 at the Supreme Court, the Law Society of Kenya challenged the Communications Authority of Kenya's installation on mobile networks of the device management system (DMS). The DMS sought to enable authorities to hear phone conversations and see mobile money transaction messages.[9]

4 Sec 30 Data Protection Act 24 of 2019 (DPA).
5 Van der Sloot (n 2) 414.
6 LK Donoghue *The cost of counterterrorism*: *Power, politics, and liberty* (2008) 186.
7 S Chesterman *One nation under surveillance: A new social contract to defend freedom without sacrificing liberty* (2011).
8 Van der Sloot (n 2) 434.
9 K Abuya 'Law Society of Kenya seeks to stop installation of spying tool by state' *techweez* 10 June 2020, https://techweez.com/2020/06/10/lsk-ca-kenya-dms-case/ (accessed 31 January 2023).

The next part of the article compares different approaches to privacy. Among liberal varieties, narrow approaches focus either on intimacy, privacy, embracing intimate information, access or decisions. Broad approaches include rights not to be pushed. They emphasise the right to be 'let alone' and relations between individuals. Privacy rights, therefore, should protect secrecy, anonymity and solitude.[10] Both these approaches protect liberty from external interference. They correspond to rule utilitarianism and act utilitarianism, respectively. Ultimately, protecting honour militates against stripping dignity away from a meaningful private life. Therefore, psychologists indicate that cultivating dignity demands more than just a secluded private place. Part 3 of what follows nonetheless demonstrates how the divergent data protection legislations of the European Union (EU) and the United States correspond to broad dignitarian and narrow utilitarian privacy conceptions, respectively. Kenya's DPA derives from the EU's 'opt-in' model. Here, before a data processor shares personal information, a data subject's prior informed consent is required. Part 4 traces major decisions of the Kenyan judiciary regarding big data, initially espousing a broad privacy approach. Subsequently, in *Communications Authority of Kenya v Okiya Omtata Okoiti & 8 Others*,[11] the Court of Appeal reverted to a narrow approach that introduces a chilling effect on individual liberty. The LSK thus sought to overturn that decision. However, the Supreme Court rejected LSK's claim, since it was neither a party before the superior nor before the appellate court. This article argues that LSK's impugned appeal arguably reflects an alternative privacy conception that does not focus on the benefit of the individual or of preventing interference, inconvenient or private disclosures 'but on the benefits to society, of maintaining a sphere of life insulated from the public gaze'.[12] Part 5 thus considers the benefits of group privacy which LSK's dismissed appeal set out to prioritise. The article concludes that African culture may proffer group privacy over the value of individualised human dignity emphasised not only in Kenya's DPA, but also international instruments, including the Draft Legal Instrument on Government-led Surveillance and Privacy (LIGSP) of the United Nations (UN).[13]

2 Surveillance ethics

2.1 Intelligence and surveillance

No agreed definition for state intelligence exists.[14] It has been defined as information theft. On the one hand, private theft is universally disapproved of as violating the moral code and thieves are subjected to savage sanctions. On the

10 Chesterman (n 7) 243.
11 [2020] eKLR (the *Mobile Telephones* case).
12 Chesterman (n 7) 244.
13 Draft Legal Instrument on Government-led Surveillance and Privacy 10 January 2018 (LIGSP), DraftLegalInstrumentGovernmentLed.pdf (accessed 31 January 2023).
14 D Omand & M Phythian *Principled spying: The ethics of secret intelligence* (2018) 9.

other hand, such information-gathering contrary to an owner's will is deemed permissible to detect and thwart threats to others or to the state, that is, to enhance public safety and national security.[15] Surveillance has two justifications. Internationally, states are suspicious about one another's intentions. Therefore, given the anarchic global legal order, surveillance is justified by neorealist international relations theory.[16] Domestically, Hobbes' *raison d'être* of the liberal nation state deems that individuals should surrender some personal autonomy to a centralised authority, responsible for public security, law and order. However, Rousseau's social contract displays tension between being human and becoming citizens. The latter are able to acknowledge in themselves and others the common conditions of being human and, thus, are willing to join with others on that footing of the common.[17] However, some individuals are free riders. Without the compulsion of law, they are incapable of remaining loyal to the sovereign. Ignoring all the duties incumbent on citizens, such self-interested individuals try to benefit from citizenship without paying the price. Thus, to obey the general will, Rousseau suggests that unwilling subjects should be 'forced to be free'.[18] For Weber, the state's administrative staff therefore possesses a monopoly over legitimate violence to enforce the political order.[19]

Rebels and criminals breaking rules challenge the prevailing constitutional arrangement's legitimacy.[20] Yet, relying on physical restraint by the police, prosecutors, judges, lawyers and jail wardens combining with prison apparatuses to repress reprisals is prohibitively expensive or even counterproductive.[21] Moreover, rather than relying on uninformed opinions of the lesser informed citizenry, the gathering of accurate information is instrumental to maintaining peace and security. People who are better informed are required to anticipate potential risks and actual threats to others and the state. Therefore, in order to prevent harms and prosecute crimes, governments are justified in establishing agencies to collect secret intelligence.[22] However, because the substantive right to privacy is primary, the executive is procedurally constrained to seek judicial evaluation of the quality of evidence against any suspect whose home is to be searched, possessions seized, family information required or communications intercepted. It is important to acknowledge data protection as a procedural right, providing regulations, methodologies and conditionalities by which substantive privacy and identity rights are effectively enforced.[23] In liberal democracies, privacy remains paramount. Hence, warrantless searches are prohibited.[24] Unless

15 Omand & Phythian (n 14) 10.
16 Omand & Phythian (n 14) 11.
17 TB Strong *Jean-Jacques Rousseau and the politics of the ordinary* (1994) 76.
18 J-J Rousseau *The social contract: Book I* (1895) chs 6-9.
19 Omand & Phythian (n 14) 14.
20 Omand & Phythian (n 14) 15.
21 WH Riker 'Public safety as a public good' in EV Rostow *Is law dead?* (1971) 383.
22 Omand & Phythian (n 14) 16.
23 NNG de Andrade 'Oblivion: The right to be different ... from oneself: Re-proposing the right to be forgotten' in A Ghezzi, AG Pereria & LV Alujevic (eds) *The ethics of memory in a digital age: Interrogating the right to be forgotten* (2014) 66-67.
24 Sec 29 Criminal Procedure Code (Chapter 75 Laws of Kenya).

the threshold of reasonable suspicion of criminality is attained, courts are not justified in issuing search warrants. By providing the minimum information needed by those who have to make security and public safety decisions, secret intelligence still plays a significant part in eliciting evidence for the criminal justice system.[25]

2.2 The chilling effect of warrantless mass surveillance

Mass surveillance inhibits people from freely expressing their thoughts, giving rise to self-censorship or creating a chilling effect. Upon becoming aware, either that they are being watched or that they are possibly watched, people also become frightened. Since they are afraid of the possible consequences of surveillance, they tend to avoid it altogether. Hence, they fear exercising their liberty of acting on their thoughts. Making people live under a cloud of anxiety violates privacy and offends dignity. The need to prohibit such chilling is evident in a line of European Court of Human Rights decisions. For instance, if a lawyer is required to report on his client's sources of money, as recommended under a Proceeds of Crimes and Money Laundering Act, then he simultaneously fears being struck off the roll of advocates or facing disciplinary proceedings for breaching advocate-client confidentiality. Consequently, even before any precipitate action has yet befallen him, he has a right to challenge such chilling legislation. Although he lodges a hypothetical court action to prevent future harm, in Europe such anxious lawyers have been held to fulfil the victim requirement.[26] Similarly, the Court has held that in Amsterdam, where certain zonal areas were subjected to surveillance, fearful people have the limited options of either frequenting them and exposing themselves to randomised searches or avoiding them altogether. By creating a chilling effect, such self-restraint violates privacy.[27] This principle extends to surveillance on the internet, whether through eavesdropping, hacking or wiretapping. The chilling effect it creates forces people to avoid using electronic media for communication for fear of having their locations detected or communications intercepted. Consider section 36 of Kenya's National Intelligence Service Act (NISA). It provides that: '[t]he right to privacy set out in article 31 of the Constitution may be limited in respect of a person suspected to have committed an offence to the extent that subject to section 42, the privacy of a person's communications may be investigated, monitored or otherwise interfered with'.[28] Furthermore, under section 42, '[w]here the Director-General has reasonable grounds to believe that a warrant under this section is required to enable the service to investigate any threat to national security or to perform any of its functions, he or she may apply for a warrant'.[29]

25 Omand & Phythian (n 14) 16-17.
26 *Michaud v France* Application 12323/11 (6 December 2012).
27 *Colon v The Netherlands* [2012] ECHR 946.
28 Sec 36 National Intelligence Service Act 28 of 2012.
29 Sec 42 National Intelligence Service Act.

Similarly, the Prevention of Terrorism Act (PTA)[30] contains unique procedures permitting targeted wiretapping for intelligence. Where there are compelling reasons for gathering data of the perpetration of a terrorism-related crime, a High Court judge may authorise wiretapping. A chief inspector of police may make a self-interested application requiring power to intercept communication. Nonetheless, dangers of generalised snooping are adequately addressed by not only requiring the police inspector-general's or the director of public prosecutions' written consent, but also imposing 10 years' imprisonment or a Kenya shilling 5 million fine (USD $ 30,800), or both, on officers who engage in wiretapping contrary to judicial authorisation.

3 The socio-ethical and legal framework of the right to privacy

3.1 Social ethical norms of privacy

Privacy establishes a niche in which individuals have the liberty to choose how they think and act. Under liberal democratic ethical and legal values, without their own informed consent, no one should be manipulated to disclose personal information about themselves to others. On the continental European variation, freedom means that when in private and public, individuals need not maintain an identical persona. Rather, one may choose to be reserved, shy and self-centred in private, yet portray an outgoing and caring public image.[31] No one should be compelled to reveal their true inner selves to others, whether concerning their mental or physical health, age, weight, attitudes, perspectives, political preferences, sexual orientation, or all and sundry matters. Personal freedom, autonomy and human dignity are fostered in the private sphere. Therefore, to enhance spiritual nature, feelings and intellect, individuals should easily express thoughts without apprehension that unwanted ears or eyes, including the government, are listening in or prying on them. An emergent chilling effect arises upon invading privacy, eroding the good life to the detriment of happiness.[32]

Privacy scholars have shown that, in liberal constitutions, one merit of privacy's social value is that opening the emotional and physical sphere in which ideas can be formulated, incubated and evaluated, fosters society's intellectual gestation.[33] Nonetheless, in Kenya, as shown in part 4.2 below, attempts to develop a privacy jurisprudence by striking down state encroachment into social space through surveillance overreach under the guise of providing national security, have been reversed on appeal. There is tension between individual privacy rights and collective security interests. While liberal democratic society as a whole is better off

30 Sec 36 Act 30 of 2012.
31 ED Cohen *Technology of oppression: Preserving freedom and dignity in an age of mass, warrantless surveillance* (2014) 3.
32 As above.
33 R Jay *Data protection law and practice* (2007).

if it facilitates the development of autonomous individuals, the state is mandated to provide collective security and requires information for that purpose. On the one hand, right to privacy proponents contend that opinions and ideas may lead to scientific, artistic and technological or political contributions from which all may benefit.[34] From this perspective, prerequisites to the development of ideas and nurturing of beliefs to develop self-confidence entail the needs to cultivate private spaces for reading, thinking, and confidential communications away from the interference of others.[35] Presumably, private citizens cannot tolerate excessive state intrusion into their lives. Therefore, by requiring the police to prove reasonable suspicion in order to obtain court warrants to search for a specific crime, conditional protections prohibit privacy invasion. Indeed, surveillance is not security and should be impartial.[36]

Is the use of generalised surveillance constitutionally permissible or does it violate privacy rights? For Nwauche, the modern right to privacy has received little legal attention in Nigeria. This creates the false impression that Nigerians can dispense with their privacy.[37] Abdulrauf thus concurs that a more effective framework is needed to protect individuals from new technological threats that have the capacity to denude one's command regarding an important component of their own personality and personal information.[38] By derogating from privacy rights, subject to requiring public participation to ratify such surveillance, Kenyan courts upheld an amendment to the 2012 PTA through introducing section 36A under the Security Laws (Amendment) Act (SLAA) for interception of private communications in the war on terrorism. More recently however, in the *Mobile Telephones* appeal, the Court seemed oblivious to the notion that generalised surveillance of disenchanted groups stifles education, personal identity and democracy that flourish in private.

Most privacy notions focus on broad individual dignity claims or narrow utility needs, rather than group privacy. For example, libertarian Mill stated that 'the only part of the conduct of anyone, for which he is answerable to society, is that which concerns others. In the part which merely concerns him, his independence is, of right, absolute.'[39] Over oneself, over their own body and mind, each person is sovereign.[40] Numerous theorists conceptualise privacy as

34 K Hughes 'The social value of privacy, the value of privacy to society and human rights discourse' in B Roessler & D Mokrosinska (eds) *Social dimensions of privacy: Interdisciplinary perspectives* (2015) 226, 229.
35 Hughes (n 34) 229.
36 B Wittes & G Blum *The future of violence: Robots and germs, hackers and drones: Confronting a new age of threats* (2015).
37 ES Nwauche 'The right to privacy in Nigeria' (2007) 1 *Review of Nigerian Law and Practice* 63.
38 LA Abdulrauf 'New technologies and the right to privacy in Nigeria: Evaluating the tension between traditional and modern conceptions' (2016) *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 120-122, 124.
39 A Dix and others 'EU data protection reform: Opportunities and concerns' (2013) 48 *Intereconomics* 268-285.
40 L Floridi 'Group privacy: A defence and an interpretation' in L Taylor, L Floridi & B van der Sloot (eds) *Group privacy: New challenges of data technologies* (2016) 83-100.

'limited access' to the self. Such notion affirms each person's desire for secrecy and for being isolated from others.[41] Consent is key. However more broadly, according to Westin, 'privacy is the claim of individuals, *groups*, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others'.[42]

3.2 Constitutional and statutory basis for regulating big data

3.2.1 Legal positivism

Privacy of individuals under the Kenyan Constitution guarantees that –

> Every person has the right to privacy, which includes the right not to have –
>
> (a) their person, home or property searched;
> (b) their possessions seized;
> (c) information relating to their family or private affairs unnecessarily required or revealed; or
> (d) the privacy of their communications infringed.[43]

To undergird this constitutional privacy protection, Parliament enacted the DPA. It reinforces compliance with the country's international obligations.[44] Such treaties include the Universal Declaration of Human Rights (Universal Declaration)[45] and International Covenant on Civil and Political Rights (ICCPR),[46] which enshrine privacy rights. They are domesticated into Kenyan law under the opening chapter on 'Sovereignty the people and supremacy of this Constitution' which states that '(5) [t]he general rules of international law shall form part of the law of Kenya.' Further '(6) [a]ny treaty or convention ratified by Kenya shall form part of the law of Kenya under this Constitution.'[47] However, under the Bill of Rights, article 24 specifically states that privacy is not absolute. Altogether, the statutory privacy clauses have some shortcomings, including ineffectively and inadequately protecting personal data.[48]

41 DK Mulligan, C Koopman & N Doty 'Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy' (2016) 374 *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, http://dx.doi.org/10.1098/rsta.2016.0118 (accessed 26 January 2022).

42 G Bhatia 'State surveillance and the right to privacy in India: A constitutional biography' (2014) 26 *National Law School of India Review* 127 (my emphasis), http://www.theregister.co.uk/2013/05/08/india_privacy_woes_central_monitoring_system/ (accessed 14 February 2023).

43 Art 31 Constitution of Kenya (Government Printer 2010).

44 M Laibuta 'The data protection officer' (2020), https://www.laibuta.com/data-protection/the-data-protection-officer/ (accessed 16 February 2023).

45 Adopted by General Assembly Resolution 217 A(III) of 10 December 1948.

46 Adopted by the United Nations General Assembly Resolution 2200A (XXI) of 16 December 1966.

47 Art 2 Constitution of Kenya.

48 N Kagotho 'Towards household asset protection: Findings from an inter-generational asset transfer project in rural Kenya' (2020) 7 *Global Social Welfare* 23.

3.2.2 Dignitarian rights theory

As alluded to above, the global commitment to human dignity is immortalised by the Universal Declaration. According to Gathii, the Universal Declaration represents 'the single most important reference point for cross cultural discussion of human freedom and dignity in the world today'.[49] Because everyone is born free and equal in dignity and rights,[50] article 22 proclaims that each member of society is entitled to the realise 'economic, social and cultural rights indispensable for his dignity and the free development of his personality'. Furthermore, the Constitution's article 28 upholds the right to have one's inherent 'dignity respected and protected'.[51] Thus, the dignitarian rights theory formulates privacy as an inalienable and sacred right that should not be derogated from. Dignity entails notions of honour to the privacy right. Hence, its safeguard attaches an intangible non-economic interest.[52] It is mostly developed in the theory of privacy protection of the dignity and moral autonomy of the human subject. Specifically, 'no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation'[53] and 'everyone has the right to the protection of the law against such interference or attacks'.[54]

3.2.3 Consequentialist ethical theory

Consequentialist ethical theory is predicated upon the capability to anticipate the consequences of an action.[55] Utilitarians are one category of consequentialists. To utilitarians, the choice that is ethically correct is the one that yields the greatest happiness to the majority. Unlike the dignitarian rights theory, utilitarianism seeks to protect an interest as opposed to the protection of a right. Generally, utilitarian ethics does not recognise privacy as an independent value, deserving of protection in its own right. Act and rule utilitarianism are two main utilitarianism types.[56] Act utilitarianism propounds the above utilitarianism definition precisely. Irrespective of personal sentiments or the societal constraints such as laws, an individual performs the act that confers profits on the majority. Conversely, rule utilitarianism also seeks surplus value for the majority, but using the fairest and most just means available. Therefore, it values justice and includes some benefit.[57] In Rawls's view, rule utilitarianism is the better ethical principle

49 JT Gathii 'Jurisdiction to prosecute non-national pirates captured by third states under Kenyan and international law' (2011) *SSRN Electronic Journal*, http://digitalcommons.lmu.edu/ilr/vol31/iss3/2 (accessed 9 February 2023).
50 Art 1 Universal Declaration(n 45) .
51 Art 28 Constitution of Kenya.
52 J Bonnitcha 'The implications of the structure of the regulatory expropriation enquiry in international investment law' MPhil dissertation, University of Oxford, 2008.
53 Art 12 Universal Declaration(n 45) .
54 Art 17(2) ICCPR(n 46) .
55 H Delany, E Carolan & C Murphy *The right to privacy: A doctrinal and comparative analysis* (2008).
56 SD Warren & LD Brandeis 'The right to privacy' (1890) 4 *Harvard Law Review* 193-220.
57 AM Lusambili & others 'Deliver on your own: Disrespectful maternity care in rural Kenya' (2020) 15 *PLoS ONE*.

to follow, as within the confines of justice to all, it promotes the greatest good for the greatest number of people.[58]

4 Alien origins of data protection legislation

4.1 Europe

Western continents on both sides of the Atlantic display divergent privacy cultures. Their respective sensibilities spawn different laws. The EU's 'command and control' model governs the handling of personal information with precise rules. A prominent governmental involvement protects the consumer's privacy. Such culture is perfectly acceptable, since Europeans valorise privacy to protect human dignity.[59] An EU Directive demands that personal data must not only 'be processed fairly and in a manner consistent with specified, explicit and legitimate purposes, maintained accurately, updated periodically, erased or rectified in a timely manner'. It must also be 'kept anonymously when identification of data subjects is no longer necessary'. Only when 'the data subject has unambiguously given his consent', may processing take place.[60] Making data processing dependent on the individual involved, and requiring a subject to express consent, adopts an 'opt-in' standard. Someone's political, religious, racial, or ethnic extraction, health status and union membership are among types of information that cannot be processed without explicit consent. Unless data controllers give their targets even more protection, the data can be erased. They should not only supply the reason – for the processing, who shall perceive the data, and specify the rights that the subject is entitled to – but also take appropriate security measures.[61] The Directive further requires member states to ensure that any personal information transmitted to a third country depends on reciprocal protection levels. Compliance is contingent upon numerous criteria ranging from the nature of information, to the legal rules prevalent in the recipient country, to the protective measures undertaken.

4.2 The United States

Free speech facilitates searching for truth. The US Constitution's First Amendment thus prohibits Congress from abridging expressive freedom.[62] This approach gives subjects a chance *not* to 'opt in' to data processing. It incorporates an 'opt-out' protocol, where individuals need to actively block collection or

58 J Rawls *A theory of justice* (1971).
59 Donoghue (n 6) 206.
60 Donoghue (n 6) 207.
61 Donoghue (n 6) 208.
62 JM Boland 'Is free speech compatible with human dignity, equality, and democratic government: America, a free speech island in a sea of censorship' (2013) 6 *Drexel University School of Law* 1-46.

commercial utilisation of personal information about themselves. Nonetheless, privacy culture stems from liberty. While security has historically been entrusted to the police, a premium is placed on preserving both individual autonomy and commercial flexibility. Consequently, self-policing supports the internet's continuing evolution and development.[63] At federal level, no comprehensive legislation is enacted to regulate data gathering and information use. Instead, the US industry combines self-regulation with governmental restraint towards dealing with information in the possession of third parties. Distinctly lower protections accorded to personal information in the US means that European entities may be prohibited from transmitting information to US actors. Therefore, under the Safe Harbor Agreement, reasonable precautions must be undertaken by US companies to ensure that data integrity information transferred from the EU to 'Safe Harbor' companies should continue without special approval.[64]

Inspired by Westin's US-based taxonomy, the present-day debate concerning online privacy typically depicts privacy as a good to be exchanged with other commodities.[65] This classification divides the privacy population into three: the fundamentalists, the pragmatics and the unconcerned. Europeans are privacy fundamentalists. They are sticklers for the highest, and consequently a utopian, standard of privacy safeguards.[66] The US are privacy pragmatics. They consent to a continuous erosion of privacy to accommodate expediency. Africans are the privacy unconcerned. They pay scant heed about their personal information. This framing serves the interests of those who profit from piercing the privacy veil. It assumes either that Africans are unconcerned about privacy or that they invest more in communal values. However, this hardly leaves room for a more flexible perspective of what constitutes group privacy and its aims. Given that all privacy essentially concerns managing boundaries along both space and informational dimensions, as some theorists suggest,[67] it is critical to grasp how such boundaries are managed within the digital domain, considering its unique substance and informational characteristics in relation to security requirements.

63 Donoghue (n 6) 208.
64 As above, 209.
65 Kagotho (n 48).
66 C Staunton and others 'Protection of Personal Information Act 2013 and data protection for health research in South Africa' (2020) *International Data Privacy Law*, https://academic.oup.com/idpl/advance-article-abstract/doi/10.1093/idpl/ipz024/5715399 (accessed 16 February 2023).
67 Z Tufekci 'Can you see me now? Audience and disclosure regulation in online social network sites' (2008) 28 *Bulletin of Science, Technology & Society* 20-36; DM Boyd & NB Ellison 'Social network sites: Definition, history, and scholarship' (2007) 13 *Journal of Computer-Mediated Communication* 210-230; GH Lapenta & RF Jørgensen 'Youth, privacy and online media: Framing the right to privacy in public policy-making' (2015) 20 *First Monday*, https://journals.uic.edu/ojs/index.php/fm/article/download/5568/4373 (accessed 14 February 2023).

4.3 Kenya's Data Protection Act

Reinforcing the constitutional provisions on privacy and informational rights, protection from the misuse of personal information is impliedly legislated in Kenya. Insisting on a trajectory of clear affirmative action, the DPA provides that the data subject's 'consent' to the processing of personal data must be an express, unambiguous, free, specific and informed expression of the data subject's desires. Apparently, to process personal data, controllers and processors are precluded from invoking implied consent.[68] However, whether or not a corporation may be able to invoke pre-ticked boxes or any other 'opt-out' consent by default, or whether a positive 'opt-in' mode shall suffice, is less clear. Hence the need for data controllers and processors alike to rethink their contemporary consent practices. 'Sensitive personal data' is more broadly defined to include proprietary particulars, marital status and family relationships, including names of the individual's parents, or spouse(s).[69]

In the application for registration, the DPA specifies the information to be supplied by the data controller and processor. They must attain adequate and minimal safeguards, security thresholds and modalities. However, this obligation is mitigated by the quantity of personal data gathered, the processing costs, and the scope of processing dynamics. Included among the application demands is a novel provision so that applicants should specify what methods are devised to indemnify data subjects from unlawful use.[70] The indemnification conditionality also signifies that data controllers and processors must account for any trespass on a data subject's rights and interests in personal data. Common data protection principles are embodied in data protection legislation worldwide. Domestically, section 25 of the DPA resembles principles applicable to international standards,[71] particularly the EU's General Data Protection Regulation (GDPR).[72]

Any individual processing the personal data of a subject is obligated to incorporate acceptable techniques for verifying age and determining consent. The selection of mechanisms may be influenced by the available technology, the ratio and the quantum of such personal data to probably be processed. A data audit, dubbed a data protection impact assessment (DPIA), may facilitate a determination of whether or not specific activities should be implemented before gathering or processing any individual's data. Where there is a 'real risk of harm'

68 G Greenleaf & B Cottier '2020 ends a decade of 62 new data privacy laws' (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=357261 (accessed 16 February 2020).

69 BJ Koops 'The trouble with European data protection law' (2014) *International Data Privacy Law* 1-14, http://idpl.oxfordjournals.org/ (accessed 9 February 2023).

70 L Determann & C Gupta 'Indian Personal Data Protection Act, 2018: Draft Bill and its history, compared to EU GDPR and California privacy law' (2018) SSRN *Electronic Journal*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3244203 (accessed 26 March 2023).

71 Koops (n 69).

72 Repealing Directive 95/46/EC (Data Protection Directive), https://en.wikipedia.org/wiki/General_Data_Protection_Regulation (accessed 27 March 2023).

to the data subject whose personal data has been acquired by an unauthorised person accessing their data, the DPA prescribes the response to be taken.[73]

5 Big decisions regarding big data

5.1 Early cases

5.1.1 The *Security Laws Amendment Act* case

In February 2015, in *Coalition for Reform and Democracy (CORD) & Another v Republic of Kenya & Another*,[74] the official opposition coalition led petitioners challenging the Security Laws (Amendment) Act's attempt to introduce section 36A to the PTA, which proposal stated that the national security organs may intercept communication for the purposes of detecting, deterring and disrupting terrorism. Furthermore, it provided that where they aim to intercept such communication, the Constitution's article 31 privacy right shall be limited.[75]

This amended provision was designed to limit the privacy right. It aimed to introduce unprecedented mass surveillance of communication by the national security agencies. Hence, its constitutionality was challenged. The state's rebuttal was that surveillance is justified in the war on terror.[76] The Constitutional Court observed that 'by widening threats of constant exposure, thus allowing intruders to pry on their personal space', surveillance 'in terms of intercepting communication jeopardises the petitioner's privacy'.[77] Nonetheless, given the scores of terrorist attacks in Kenya's recent past, the impugned provision was of genuine public interest. The privacy right, therefore, had to be balanced against common good exigencies.[78] All five judges concurred that there were sufficient safeguards ensuring that the limitations placed on privacy rights by intercepting communication and conducting searches would not be undertaken arbitrarily and using a widespread scope.[79] Consequently, limiting privacy was upheld as justified in a free and democratic society, for detecting, disrupting and preventing terrorism.[80] Simultaneously, in an apparent bid to stem the tide of generalised surveillance, SLAA amended section 36 of NISA to permit warranted derogations from privacy during investigations and monitoring of a person 'who is subject to investigation by the service'.[81] Ironically, however, immediately after this case,

73 Staunton and others (n 66).
74 [2015] eKLR.
75 *CORD* (n 74) 55-56 para 65. It introduced sub-secs 36(4), (5) & (6).
76 *CORD* (n 74) 59 para 298.
77 *CORD* (n 74) 57 para 290.
78 *CORD* (n 74) 60 para 302.
79 *CORD* (n 74).
80 *CORD* (n 74) 61 para 308.
81 Sec 55 Security Laws (Amendment) Act 2014.

as demonstrated in part 5.2.2 below, a broad privacy approach was adopted by courts constraining data collecting and monitoring. Only recently have the courts reverted back to a narrow approach permitting generalised surveillance and, thus, failing to avert big data's chilling effect.

5.1.2 The *Nubian Rights Forum* case

In *Nubian Rights Forum & 2 Others v Attorney General & 6 Others; Child Welfare Society,*[82] several organisations complained against the destruction, deletion or loss of vital records containing personal data, and of identity theft and fraud. They expressed fear of malicious utilisation of the information, false entries, mismatching information and hacking through cybercrimes. High Court justices Ngugi, Nyamweya and Korir JJ (as they then were) agreed that the state's proposed DNA collection and global positioning system (GPS) co-ordinates for identification purposes were invasive, unnecessary, and unauthorised by the impugned enabling legislation. Because data protection was not guaranteed, the scheme violated the Constitution's article 31 privacy rights.

5.1.3 The *HIV* case

In 2015, President Uhuru Kenyatta ordered all county commissioners and three cabinet secretaries for the Ministries of (i) Interior and Coordination of Government; (ii) Education, Science and Technology; (iii) Health; as well as (iv) the National AIDS Council, to gather updated data and report on all school-going children living with HIV and AIDS.[83] However, four petitioners were apprehensive, first, that in violation of the HIV and AIDS Prevention and Control Act,[84] the order would result in forced or compulsory testing, second, that it would also result in forced disclosure of information about one's HIV status, contrary to privacy rights, equality freedoms, as well as the targeted persons' dignity.[85] The respondents rebutted by saying that the President's impugned directive aimed to provide HIV-positive persons and the private sector with necessary political will. Furthermore, that this data would also increase limited access to anti-retrovirals (ARVs) for school-going children and youths who suffer stigma and exclusion for living with HIV.[86] Moreover, several guidelines provide for privacy and confidentiality in implementing services, research and data gathering in different situations.[87] Indeed, they countered that the names of people with chronic care conditions, not only persons living with HIV, are already available in respective hospital and HIV care clinic registers, for

82 [2020] eKLR (*Nubian Rights Forum* case).
83 *Kenya Legal and Ethical Network on HIV & AIDS (KELIN) & 3 Others v Cabinet Secretary Ministry of Health & 4 Others* [2016] eKLR.
84 14 of 2006.
85 *KELIN* (n 83) para 14.
86 *KELIN* (n 83) para 30.
87 *KELIN* (n 83) para 32.

follow up, attention and ARV treatment.[88] However, a UN expert reinforced the petitioners' perspective that the unlawful disclosure of an individual's HIV status contravenes their privacy rights.[89]

Defining privacy to include 'those matters whose disclosure will cause mental distress and injury to a person', Lenaola J (as he then was), approaching privacy broadly, held that the Constitution's article 31(c) protects against the unnecessary revelation of information regarding family or private affairs.[90] Articulating privacy as a right to live one's own life with minimum interference, he held that it also restricts the gathering, utilisation and disclosure of private information.[91] Consequently, the judge struck down the directive as unconstitutional. It violated the petitioners' constitutional privacy rights and as such was not in the child's best interests. Instead, he ordered that the children's names should be stored in a public document in a way that delinks their HIV statuses from themselves.

5.2 The *Mobile Telephones* case

5.2.1 The High Court

In April 2018, in *Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others*[92] the High Court held that phone records should not be deployed for generalised surveillance. Mativo J (as he then was) approached privacy as a broad fundamental human right that is 'central to the protection of human dignity and forms the basis of any democratic society'.[93] Yet, this article notices that nowhere is any right to privacy expressly enshrined in the African Charter on Human and Peoples' Rights (African Charter). It is only implied by the collective self-determination right.[94] Nonetheless, the judge recognised that domestically '[t]he right to privacy embodies the presumption that individuals should have an area of autonomous development, interaction, and liberty, a "private sphere" with or without interaction with others, free from arbitrary state intervention and from excessive unsolicited intervention by other uninvited individuals'.[95] Therefore, surveillance and censorship that restrict privacy may only be justifiable when 'prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued'.[96] Furthermore, the emergence of new challenges is exemplified by the context of an information based world. The judicial task in the information era, where technology infiltrates almost every dimension of our activities, is to

88 *KELIN* (n 83) para 33.
89 *KELIN* (n 83) paras 43-50.
90 *KELIN* (n 83) para 68.
91 *KELIN* (n 83) para 69.
92 [2018] eKLR.
93 *Okoiti* (n 92) 16 para 63.
94 V Bermingham, J Hodgson & S Watson *Nutshells tort* (2014).
95 *Okoiti* (n 92) 16 para 63.
96 As above.

confer constitutional meaning to individual liberty in the global network. Kenya's Constitution protects privacy as a basic principle. Consequently, in a digitised world the court should be responsive to the necessities of surveillance abuse and the possibilities and risks to liberties.[97]

Mativo J declared that since the mobile network owners were excluded from consultations in policy formulation and implementation, the government's intended telephone surveillance policy was constitutionally invalid as it conflicted with the right to privacy. He agreed with Okoiti that by installing a communication surveillance system, styled as the 'device management system' (DMS), on mobile telephone networks, 'millions of subscribers and the general public whose records are held' were endangered. Clearly, to monitor the population by defying the constitutional protection of privacy, the government had a hidden agenda. To Okoiti's chagrin, the DMS device would spy or snoop on the general population and harvest and stock subscribers' personal data. This would facilitate the state's access, collection and retention of subscribers' communication data. However, according to the Communications Authority of Kenya (CAK), the DMS system was meant to fight fake and offending devices. Ultimately, the High Court prohibited CAK from effecting its decision to establish connectivity between the DMS and mobile phone operators.[98]

5.2.2 The *Mobile Telephones* case: Court of Appeal

In *Communications Authority of Kenya v Okoiti & 8 Others*[99] the CAK successfully appealed. Ouko J (as he then was), Koome (afterward Chief Justice) and Musinga JJA considered three issues: first, whether by intercepting and recording of communication and mobile data, the DMS installed by CAK would signal an era of public regulation and espionage on peoples' privacy; second, whether the CAK adequately allowed public participation in the development and installation of the DMS; third, whether the dispute was prematurely taken to court.[100] They recalled that 'since its advent in Kenya in early 2000', the regulation of mobile communication 'was guided by the world-wide global system for mobile communication (GSM)'. Because Kenya agreed, by various international agreements, 'to identify mobile communication devices that have been manufactured with regard to GSM standard', this process is regulated. Therefore, mobile phones must bear a 15-digit serial number called the international mobile equipment identity (IMEI). Such identification mark of quality 'is issued by Global System for Mobile Communications Association (GSMA) which maintains a global central database containing numbers of millions of mobile devices, ie mobile phones, tablets, data cards etc known as IMEI Database'.[101]

97 *Okoiti* (n 92) 16 para 64.
98 *Okoiti* (n 92) 38 para 163.
99 *CAK* (n 11).
100 *CAK* (n 11) 2 para 1.
101 *CAK* (n 11) 2 para 3.

Moreover, world over the theft of mobile handsets and the proliferation of fake and illegal phones came into sharp focus for regulators. Simultaneously, pawns handling counterfeit handsets became more tech-savvy and began cloning genuine IMEI numbers to the dud models, which made discovery more difficult.[102] Consequently, when compared with the GSMA IMEIs database whitelist and in the event of disconnection, counterfeit devices looked legitimate.[103] CAK also faced escalation of SIM boxing, the next horizon for combating fake devices.[104] Effectively, in contravention of section 24(1) of the Kenya Information and Communications Act,[105] SIM boxing operators evade licence fee payments which require that they also do not pay the requisite taxes for eliminating international traffic within Kenya, thus inflicting considerable revenue losses of national capital. The only records that are held by the local operators from a call originating from SIM boxing is the domestic number used in the operations, making SIM boxing a fulcrum for criminal enterprises as the actual source of the audio calls is untraceable. Additionally, CAK received complaints from country operators within East Africa, particularly Rwanda, that the SIM boxing operation in Kenya was being utilised to stop international traffic, causing revenue losses.[106]

CAK's appeal succeeded on technicalities. Procedurally, because Okoiti's petition consisted of 'generalised allegations' that were 'wholly predicated on unsubstantiated statements taken from newspaper reports and statements made by unnamed technical experts'. It was 'slovenly drawn'. In pertinent part, the petition alleged that the state mentioned nothing concerning the system's potential for tapping telephone calls and texts and also peeping into all mobile cash transfers and how it will safeguard individual privacy, once the information is not only gathered by CAK but also hived off by third parties, not limited to the state's law enforcement and other public actors.[107]

Okoiti's rejected evidence comprised newspaper snippets with exaggerated headlines, such as 'Bold plan to spy on all calls, texts rolled out from Tuesday next week, if mobile firms comply, someone other than your provider will be able to access your call, text and money transfer data';[108] and also 'Big Brother could start tapping your calls, texts from next week'.[109] Altogether, Okoiti's supporting depositions on accusations of what scared him may occur, were conjectures or, at best, unconfirmed sources of information. For example, his petition at paragraph 9 speculated that '[t]echnical experts have pointed out that while there would be no concern over the access to the International Mobile Subscriber Identity, which is a unique number identifying a mobile phone subscriber, other access like

102 *CAK* (n 11) 2 para 5.
103 *The Standard* cited in *Okoiti* (n 11) 2-3 para 5.
104 *CAK* (n 11) 3 para 5.
105 2 of 1998.
106 *CAK* (n 11) 3 para 6.
107 *CAK* (n 11) 15 para 37.
108 *Daily Nation* 17 February 2017.
109 *CAK* (n 11) 15 para 38.

home location register raise concerns'.[110] Therefore, the appellate judges allayed his apprehension that the state's motive was to engage in espionage.

In sum, allegations of surveillance abuse by unscrupulous mobile operators also required to strike a balance between securing the privacy right without infringing it.[111] Consequently, the appellate judges unanimously concluded that 'there was no concrete evidence that the DMS was going to spy or intrude on private communication' and, moreover, 'that there were genuine issues raised by MNOs which were still being discussed'. The Court of Appeal ordered, first, that pursuant to its commission of developing a DMS system, the CAK should not halt ongoing consultations among stakeholders and MNOs in order to finish 'the technical and consumer guidelines on the DMS'; second, that such 'guidelines/ regulations should be subjected to public participation'.[112]

5.2.3 The *Mobile Telephones* case: The Supreme Court

Despite the Court of Appeal judges ignoring the DMS constitutionality issue and its threat to privacy rights of millions of mobile telephone subscribers, the Supreme Court faulted LSK.[113] Moreover, it also ignored alarm bells sounded by telephony giant Safaricom that the DMS will enable the CAK to monitor other customer data held by the telecoms operators. Conversely, insisting that the monitoring devices can only find and save the special identification number of mobile devices and assigned subscriber numbers, CAK emphatically denied that the technology had the capacity to access the phone records, locations, and mobile cash transfer particulars of subscribers. Yet, given that LSK was alien to both the High Court and Court of Appeal proceedings, Mwilu DCJ, Ibrahim, Wanjala, Ndung'u and Lenaola SCJJ declined to deal with substantive issues concerning its challenges to data protection law. Neither had Okoiti appealed to the Supreme Court. Therefore, what the apex judges' opinions on the merits may have been, remains moot. Miffed by the order of costs made against it while desperately seeking to execute its own statutory mandate to 'uphold the Constitution and administration of justice', LSK moved to the East African Court of Justice. The advocate's body 'complained over the Supreme Court decision to exclude participants who are not parties to a case from lodging an appeal'.[114] Meanwhile, other civil society activists remained unimpressed with the Court of Appeal's controversial decision and are exploring alternative means of circumventing it.

110 *CAK* (n 11) 16 para 39.
111 *CAK* (n 11) 19 para 47.
112 *CAK* (n 11) 21 para 54.
113 S Kiplagat 'Regulator allowed to install mobile phone spying gadget' 28 April 2023, https://www.businessdailyafrica.com/bd/economy/regulator-allowed-to-install-mobile-phone-spying-gadget--4215610 (accessed 28 April 2023).
114 J Wangui 'Kenya lawyers take Supreme Court to EACJ' *The East African* 26 June 2023, https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-lawyers-take-supreme-court-to-eacj-4282206 (accessed 11 October 2023).

5.2.4 The *Huduma Namba*[115] case

High Court

In *Katiba Institute v Attorney General*,[116] a non-governmental organisation (NGO) challenged the Information, Communications and Technology Cabinet Secretary, Mucheru's 18 November 2019 rollout of a new identity card, known as 'Huduma card', which was proposed as the primary data source on every citizen and foreigner. It was to be issued upon gathering and processing the data subject's personal data.[117] Was such collection and processing of personal data under the National Integrated Identity Management System (NIIMS) subject to DPA?[118] Despite the government having spent more than Sh 10 billion (US $74 626 870) for failing to comply with DPA, Ngaah J nullified the card's launch. Prior to collecting and processing personal data for the Huduma cards, the government should have conducted a data protection impact assessment (DPIA) to identify any risks, such as contraventions to privacy and data loss.[119] Moreover, some Kenyans who lack identity cards may be excluded from the roll-out. Since processing under NIIMS, including the capturing of children's biometrics and data, and was likely to result in high risk to people's rights and liberties, the High Court compelled the state to first conduct the requisite DPIA.[120] Evidently, the judge's decision appears based on promoting board dignitarian privacy concerns. This approach elevated the threshold required to justify societal ouster of privacy rights.

Court of Appeal

In *Attorney General* v *Katiba Institute*,[121] Data Protection Director-General Kassait and Attorney-General Kariuki objected that the Katiba Institute did not possess any data and, thus, was precluded from being an aggrieved person.[122] The Court of Appeal, however, dismissed the government's objection to the hypothetical claim and its plea to continue issuing Huduma Namba cards without conducting impact assessment on data protection. Justices Murgor, Mbogholi-Msagha and Laibuta JJA questioned the state's failure to register Kenyans afresh and conduct a DPIA, as required by DPA. They criticised the government for

115 Swahili for 'service number'.
116 *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 Others; Katiba Institute & Another (Ex parte); Immaculate Kassait, Data Commissioner (Interested Party)* Judicial Review Application E1138 of 2020 [2021] KEHC 122 (KLR) (Judicial Review) (14 October 2021) (Judgment).
117 *Katiba* (n 116) 2.
118 *Katiba* (n 116) 3.
119 *Katiba* (n 116) 6-7 para 23.
120 S Kiplagat 'High Court declares Huduma Namba illegal' *Business Daily* 14 October 2021, https://www.businessdailyafrica.com/bd/news/high-court-declares-huduma-namba-illegal--3582926 (accessed 6 March 2023).
121 *Mucheru & 2 Others v Katiba Institute & 2 Others* Civil Application E373 of 2021 [2022] KECA 386 (KLR) (4 March 2022) (Ruling).
122 K Muthoni 'Court dismisses plea to roll out Huduma Namba over data safety' *The Standard* ,https://www.standardmedia.co.ke/national/article/2001439648/court-dismisses-plea-to-roll-out-huduma-namba-over-data-safety (accessed 7 March 2023).

belatedly enacting DPA in the hope of salvaging the Kshs 10.6 billion expended on the data collection exercise. They agreed with Justice Ngaah that the state ought to have first enacted a data protection law, followed by amending the Registration of Persons Act, before rolling out the Huduma Namba exercise. For creatively upholding the activists' hypothetical claims, thereby reverting to a broad privacy approach in departure from Okoiti's *Mobile Telephones* precedent, they endorsed the judge. Kenyan government services are increasingly offered through digital platforms, such as e-citizen. With the proposed new 'Maisha numbers' allocated by the government, national ID cards will gradually be replaced by a transition to digital identity.[123] However, as shown below, just as the theft of Kenyans' irises may expose customers to direct marketing, it is possible that such data, if insecure, may interfere with democratic choices.

5.3 WorldCoin's unauhorised bio-data mining

In April 2023, Data Protection Director-General Kassait discovered that Worldcoin had been collecting personal information from Kenyans. Although Worldcoin had applied for a certificate of registration as a data controller, it neither complied with sections 18 and 19 of the DPA, nor was authorised to operate in Kenya.[124] Yet, hundreds of thousands of Kenyans flocked to the Kenyatta International Convention Centre and several Nairobi malls to have their eye balls captured by parent company, Tools for Humanity and Sense Marketing Limited, traded-off for Kshs 7 000 (US $50) worth of crypto currency.[125] Using their phone application, cryptocurrency and 'orb' scanner, these foreign corporations scanned Kenyans' bio-metric data for over a year. Despite a world class DPA, Worldcoin ignored the DP Commission's instructions to cease invading individuals' privacy by harvesting biometric data, in the absence of proper and convincing justification.[126] It had neither a legal basis for gathering sensitive personal data or the transferring of personal data, nor proof that those people who had their irises scanned had consented to the disclosure of their personal data. Pending the conclusion of investigations, Judge Prof Nixon Sifuna not only prohibited Worldcoin from gathering Kenyans' data, but also ordered it to preserve the information already gathered from 19 April 2022 to 8 August 2023.[127] The hearing continues.

123 Citizen Team 'Gov't to begin Maisha Namba Digital ID awareness drive this weekend' *Citizen* 15 September 2023, https://www.citizen.digital/news/govt-to-begin-maisha-namba-digital-id-awareness-drive-this-weekend-n327456 (accessed 1 November 2023).

124 F Chandianya 'Data commissioner unaware how many Kenyans scanned eyes in Worldcoin' *NTV* 15 August 2023, crazehttps://ntvkenya.co.ke/news/data-commissioner-unaware-how-many-kenyans-scanned-eyes-in-worldcoin-craze/ (accessed 1 November 2023).

125 I Houghton 'Protect Kenyans from digital data trafficking' *Amnesty International* 21 August 2023, https://www.amnestykenya.org/protect-kenyans-from-digital-data-trafficking/ (accessed 1 November 2023).

126 A Njanja 'Worldcoin ignored initial order to stop iris scans in Kenya, records show', https://techcrunch.com/2023/08/15/worldcoin-in-kenya/ (accessed 1 November 2023).

127 S Kiplagat 'Keep off Kenyans' eyes, court orders Worldcoin as probe on' *Business Daily* 15 August 2023, https://www.businessdailyafrica.com/bd/economy/keep-off-kenyans-eyes-court-orders-worldcoin-as-probe-on--4335544 (accessed 1 November 2023).

6 Group privacy, regional and emerging international counter-surveillance and privacy instruments

6.1 Group privacy

Appertaining to big data analytics, it was Floridi who pioneered the group privacy idea.[128] In his thesis, groups have privacy rights that are irreducible to the privacy of individual members of such groups. In response to big data technology advances, group privacy, therefore, should also be a goal of privacy control. Nonetheless, an absolute right, whether of individuals or groups, to *inferential* privacy, is unrealistic.[129] Under a narrow conception, privacy is essential for restricted access to oneself or information about the self, the right to be left alone.[130] In digital interactions, privacy may be understood as an all-embracing right that safeguards virtually every component of identity, personhood and dignity.[131] Because *homo sapiens* as citizens are social beings and, further, because human joy requires that individuals expose their inner selves to one another, therefore, this is a consequentialist approach. Effectively, by joining groups, individuals violate their own privacy and to keep within the group what was revealed, rely on those with whom they associate not to reveal their shared secrets. Such group privacy safeguards people's external, as opposed to their internal, space. This expresses their gregarious nature, rather than their desire for complete isolation.[132] Nonetheless, group privacy remains an individual right. In situations where groups may, nonetheless, be easily identified and targeted, Floridi highlights the risks emerging from opening *anonymised* personal data to public access.[133] Practically, every form of generalised knowledge may subject groups to special risks. Consider the discovery that smoking causes cancer, exposing all smokers to enhanced insurance premiums.[134] Similarly, in virtue of generalised knowledge extracted from a few of a group's individuals, *inferences* about other individuals in the group may be drawn. An entity's individual or collective *inferential* privacy, is a metric of the logically valid inferences, regarding someone's *sensitive features*, that can neither be made nor derived from the available data.[135] Sensitive features 'can be defined as features which most individuals in a given society at a given time do not want widely known about themselves'.[136]

128 L Floridi 'Open data, data protection, and group privacy' (2014) 27 *Philosophy and Technology* 1-3.
129 M Loi & M Christen 'Two concepts of group privacy' (2020) 33 *Philosophy and Technology* 207-224.
130 Warren & Brandeis (n 56).
131 M Hildebrandt 'Balance or trade-off? Online security technologies and fundamental rights' (2013) 26 *Philosophy and Technology* 357-379.
132 EJ Bloustein *Individual and group privacy* (2003).
133 Floridi (n 40) 98.
134 L Taylor 'Safety in numbers? Group privacy and big data analytics in the developing world' in Taylor and others (n 40) 14.
135 Loi & Christen (n 129) 218.
136 Loi & Christen (n 129) 219 citing WA Parent 'Privacy, morality, and the law' (1983) 12 *Philosophy and Public Affairs* 269-288.

An algorithmically-sorted group should, if its members so desire, possess a right to fashion their identity and advance their common interests.[137] It might as well be conceded that individuals in such group may share an interest *not* to be amalgamated into a collective, for example, a group that is discriminated against. However, in such specific society, the group interest in issue is a mere shared interest, an aggregate of identical individual interests. At least in design or in conception, it is not a collective interest in a way that presupposes the prospects of group interaction.[138] Rather, what big data analytics threaten is specifically the *inferential* privacy of individuals that are characterised by sensitive features common to all-inclusive groups. The allegedly special danger facing the *inferential* privacy of groups (compatible with the anonymity of individuals within such groups) may be reduced to a more pervasive difficulty regarding destructive utilisation of generalised knowledge. Such knowledge may affect far more people than the few who facilitated the acquisition of such knowledge.[139] Not all types of privacy can be protected by giving individuals, or groups, rights to regulate information. On the contrary, *inferential* privacy needs a notion of the societal impact of innovation. In this article's argument, invoking rule utilitarianism, LSK's challenge against CAK's generalised surveillance may be seen as objecting to client, patient or customer communications that are in possession of telephone operators, being generally shared with the state by the regulator. Generalised eavesdropping may cause advocates as a group to 'chill' from utilising 'leaky' mobile telephones for fear of breaching ethical duties prohibiting them from divulging client information to third parties without consent.

6.2 Regional comparisons

The African Charter[140] lacks an express privacy right. Nonetheless, privacy may be *inferred* as a derivative of the universal prohibition on arbitrary killing. Locke was of the view that natural laws exist, one of these being the right to life.[141] The Western right to privacy originates in individualism, since each person possesses a right to self-determination. This means that they have the right to choose which aspects of their personal lives to reveal and which aspects to conceal. Conversely, from an African perspective, privacy is perceived as a group right, since '[a]ll peoples shall have the right to existence. They shall have the unquestionable and inalienable right to self-determination. They shall freely determine their political status and shall pursue their economic and social development according to the policy they have freely chosen.'[142] In this context, self-determination is a

137 B van der Sloot 'Do groups have a right to protect their group interest in privacy and should they? Peeling the onion of rights and interests protected under article 8 ECHR' in Taylor and others (n 40) 159-173.
138 DG Newman 'Collective interests and collective rights' (2004) 49 *American Journal of Jurisprudence* 140.
139 Loi & Christen (n 129) 222.
140 African Charter on Human and Peoples' Rights concluded at Nairobi on 27 June 1981.
141 Van der Sloot (n 6).
142 African Charter (n 140).

persisting right – one that is not successfully actualised by decolonisation or individualisation and the disappearing of racist regimes. Although the right to secede is not expressly enshrined by the African Charter, it also is not prohibited. Hence, self-determination is exercised by groups, rather than individuals.[143]

Nwauche reflects that, in the Nigerian Constitution, there may be a generalised and specialised understanding of privacy. On the one hand, the provision's general right is 'the privacy of citizens'. Conversely, the phrase 'their homes, correspondence, telephone conversations and telegraphic communications' lists specific instances of the general right. Furthermore, applying principles from the torts of breach of confidence and of privacy,[144] these privacy perspectives create a dilemma, namely, if respect for a private life is defined too widely, it could lead to an undesirable restriction on the freedom of the press to report and comment on matters of public importance. This has concerned English courts.[145] Abdulrauf thus concludes that Nigeria's narrow constitutional provision may be an insufficient legal instrument for individuals to enforce their right to control the access and utilisation of personal information.[146]

6.3 International initiatives

In 1980, a White Paper by Lord Diplock confirmed that in the UK 'interception might be undertaken only with the Secretary of State's authority given by a warrant of his own hand'.[147] Secret surveillance was justified by forwarding of threats and opportunities. Spying maintains power relative to competitors. Hence, in *Privacy International v Secretary of State*[148] the Court of Appeal dismissed an appeal by numerous NGOs claiming that the government's 'Guidance on the Use of Agents who Participate in Criminality' was unlawful. In its early responses, European Court jurisprudence rejected hypothetical claims regarding damages that are yet to materialise, on grounds that the data subject is unsure and could not substantiate his claims. Since the claimant could not show that he himself had been a direct or indirect victim of a violation of the European Convention on Human Rights, a public interest litigation basis was rejected.[149] However, with the emergence of big data decisions, claimants with hypothetical grievances now attain recognition and remedies. For example, in *Klass v Germany*, there existed a legislative framework governing the use of covert intelligence, potentially affecting all users of postal and telecommunications services. Similarly, in *Hilton v UK*,[150] the Court held that there had to be at least reasonable likelihood that

143 MK Addo 'Political self-determination within the context of the African Charter on Human and Peoples' Rights (1988) 32 *Journal of African Law* 182-193.
144 Nwauche (n 37) 84.
145 Bermingham (n 97) 269-270.
146 Abdulrauf (n 38) 120-121.
147 Delany and Others (n 55) 46.
148 [2021] EWCA Civ 330; 2 WLR 1333.
149 Van der Sloot (n 2) 417.
150 [1978] 2 EHRR 214.

the Security Service has compiled and continues to retain personal information regarding the claimants.[151] Nowadays it is accepted, in Europe at any rate, that the mere existence of an intrusive law at domestic level, may lead to interference with the right to privacy contravening the European Convention.[152] Notwithstanding the fact that some claimants were yet to be subjected to surveillance measures, the courts have struck down surveillance laws and practices to alleviate a chilling effect. Clearly, the Kenyan Court of Appeal decision in the *Mobile Telephones* case is irreconcilable not only with EU, but also global, data protection laws.

The UN's draft Legal Instrument on Government-led Surveillance and Privacy (LIGSP) crystallised from meetings and correspondence between the MAPPING project and several stakeholder categories designing the development and utilisation of digital technologies. They comprise leading global technology companies, experts experienced in working within civil society, law enforcers, intelligence services, academicians and diverse multi-stakeholder community members shaping the internet and the transition to the digital age.[153] Emergent consensus is that human rights should be considered as a single entity, encompassing the rights of people to develop their lives and personalities in a similar manner to the rights of crime victims and of individuals to inhabit safe and secure surroundings.[154] In the digital age, it emphasises the promotion and protection of human rights.[155] It rejects bulk interception carried out by police. However, the digital technologies used to conduct surveillance are becoming increasingly identical. Sometimes multiple state agencies use them or they are provided by third-party vendors. Thus, LIGSP aims at developing provisions that fully defend, respect and preserve human rights not limited to public safety, fair trial rights and victim's rights, but also privacy and personality rights. Mimicking the EU's stance, LIGSP thus propounds that all human rights stem from human dignity. It has become highly important to construct confidence and trust in the internet, including regarding freedom of expression, privacy and other human rights. Thus, the online sphere's potential as a facilitator of development and creativity is attainable, through mutual cooperation between governments, global institutions, civil society, the private sector, the technical community and academia.[156] Focus on expressive freedoms and privacy is purposive.[157] It is essential that individual human rights are inalienable, universal and indivisible. Rather than trading-off between rights, means of their fortification and consolidation should be pursued, ultimately elevating human dignity.[158] The costs of peace are subject to sudden, intense 'fluctuations of anger, love,

151 Van der Sloot (n 2) 421.
152 *Malone v United Kingdom* [1984] ECHR 10; *PG & JH v the United Kingdom* Application 44787/98 Judgment 25 September 2001.
153 LIGSP (n 13) 2.
154 As above.
155 LIGSP (n 13) 3.
156 LIGSP (n 13) 5.
157 LIGSP (n 13) 6.
158 Art 1(9) (n 13).

contentment and aggravation'.[159] Therefore, in balancing of individual privacy with societal interests such as security, the individual right will lose. Instead, intuitionism endorses legal pluralism that accepts all,[160] including group, privacy. A DPIA may create conditions for a quantitative survey of public opinion. Politicians need to persuade the general citizenry to recognise whether to value digital surveillance to repress crime or prefer to uphold the dignity of privacy. A middle ground created, for example under sections 36 of the PTA, empowers senior police officers who reasonably suspect that terrorism-related offences have been committed to approach the High Court for an order to intercept communications. Robust safeguards precede either ordering a communications service operator to wiretap and retain specified communication, or authorising the police's entry onto premises to install interception and retention devices and to remove intercepted communications. Violating privacy contrary to court orders attracts severe penalties. PTA's section 36 is narrower than NISA's section 36. The former prescribes procedures regulating specific interception of communications to detect, deter and disrupt terrorism, thus facilitating limited surveillance conferring relatively broader privacy protections. Similarly, covert investigations targeting reasonable suspicion of other serious organised crimes are preferable to the *Mobile Telephones* precedent authorising generalised surveillance that narrows privacy, even chilling group privacy.

7 Analysis of findings

Kenya's DPA purposes to protect personal information from being shared to the detriment of data subjects. However, that Act is too narrow with respect to privacy limitations on the ground of privileging national security. Its professed consequentialism advocates a narrow approach for judicial oversight on privacy, thereby condoning surveillance. DPA exempts the processing of personal data by public authorities in the public interest or for functions which include national security or crime prevention.[161] Consequently, the power to collect or monitor is widely permissible for the personal data found in a public record or where the gathering of data from another source is essential to prevent, detect, investigate, prosecute and punish crime.[162] The Director-General of National Intelligence Service's section 36 discretion to collect personal data through surveillance is subject to obtaining special judicial warrants upon showing reasonable suspicion. However, given the emergence of big data intelligence surveillance, the state may unsuspectingly gather personal data unrelated to national security or suspicion of crime.

159 Riker (n 21) 381-382.
160 Chesterman (n 7) 244.
161 Secs 30(2)(b)(iv)-(vi) DPA (n 4).
162 Secs 28(2)(a)(i) & (f) DPA (n 4).

Because individuals cannot articulate big data's diffuse personal harm, civil society activists have lodged public interest litigation claims against the government and even corporations accused of conducting inadvertent or intentional generalised surveillance on citizens.[163] DPA's sections 28 and 30 allowing governmental intrusion into privacy are general and do not meet the constitutional necessity criterion. Invoking section 31 in *Huduma Namba*, by directing the data protection commissioner to conduct a DPIA, Judge Ngaah therefore insisted on public participation preceding roll-out. This article's contribution is that a DPIA provides an avenue for citizens' oversight enforcement of group privacy. It enforces the need to ensure that prior informed consent from data subjects as a whole is obtained as a procedural check against executive surveillance or interception of personal data. On the one hand, this retains the broad privacy approach adopted in the *Nubian Rights Forum* and *HIV* cases, requiring that surveillance should not be linked to specified persons. However, judicial oversight is limited to the initial phase and does not extend to the subsequent process, whereby personal information that is unrelated to national security may be collected while collecting the warranted data. On the other hand, notwithstanding that legislation or practice creates a reasonable likelihood that a data subject may be harmed, in the *Mobile Telephones* case the Court of Appeal was unwilling to allow for speculative claims decrying consequent chilling contingent upon generalised surveillance. Yet, given that free rider problems constrain individuals from producing public goods, civil society groups and non-legal persons are better suited than individuals to monitor generalised surveillance. Although there are constitutional and statutory bases for limiting privacy rights, there is ambiguity in big data's regulation. This article considers the applicability of data protection laws regulating big data's impact on consent by affected data-sharing subjects or victims. Based on interference with the privacy of advocate-client relationships, the LSK as a group challenged the CAK's sharing of big data. Ultimately, the Supreme Court dismissed LSK's appeal on a procedural technicality, thereby obliterating the focus on the victim requirement evinced by the 'chilling effect'.

On a group privacy concept, judicial oversight of governmental surveillance may require law enforcement agencies to ensure that the form of surveillance, although focused on a particular suspect, does not give rise to generalised surveillance. Assessment of public opinion should be preceded by a DPIA, during which affected groups may choose whether or not to 'opt in', based on objective information.[164] Individuals and groups require rights to correct data, to be forgotten and to have legal remedies. Besides the DPA, there are other statutes that broadly address some digitisation threats,[165] ranging from the NISA[166] to the

163 'A new lawsuit accuses meta of inflaming civil war in Ethiopia' *Wired* 13 December 2022, https://www.wired.com/story/meta-hate-speech-lawsuit-ethiopia/ (accessed 14 April 2023).
164 *CAK* (n 11).
165 G Mutung'u 'Kenya country report' in T Roberts and others (eds) *Surveillance law in Africa: A review of six countries* (2021) 72-101.
166 Sec 36 NISA (n 28).

Computer Misuse and Cybercrimes Act.[167] The legislature could go further by restricting the forms of technology that are used for surveillance. To prevent the government from infringing on the privacy of innocent individuals in the process of investigations of criminal suspects, there should be proper legislation to incorporate accountability, transparency and adequate oversight of surveillance systems. On the globally-dominant dignitarian model, big data collection and surveillance are viewed as unconstitutional. The burden should be placed on data processors and controllers to prove that intelligence surveillance tools, such as closed-circuit television (CCTV) cameras, ensure that third party access is highly restricted and does not violate individual or group privacy. Nowadays, given technological advancements, surveillance exceeds telecommunication channels. Yet, interception authorised under the PTA is restricted to the perpetration of terrorism-related offences or information pertaining to 'the whereabouts of the person suspected by the police officer to have committed the offence'.[168]

Data protection law confers procedural protection of substantive privacy and identity rights. The courts should strictly evaluate every application by law enforcement agencies for surveillance or search and seizures. Broad approaches to privacy demand judicial scrutiny of the surveillance purpose to ensure that such surveillance is the least restrictive in the circumstances. Curiously, in Okoiti's *Mobile Telephone* case, the Court of Appeal invoked the obsolete requirement of insisting that litigants should demonstrate individual harm by generalised surveillance. That decision was remarkably oblivious to the inherent harm that any generalised surveillance creates. However, Okoiti did not move to the Supreme Court as an aggrieved individual to reverse the Court of Appeal's narrow conception of privacy and, further, LSK's attempt to articulate grievances afflicting group privacy was technically barred. Parliament should urgently legislate to address the chilling effect that new technologies impose on both individual and group privacy. At stake is the allegedly special threat against the *inferential* privacy of groups characterised by sensitive features common to open-ended groups. Kenya's data protection laws require strengthening to adequately protect collective citizens' privacies and group identities from generalised digital surveillance.

The courts have rejected complaints that neither a privacy impact assessment nor public participation preceded the *Maisha Namba* rollout, thereby compromising citizens' biometric and biographical data.[169] In criminal procedure, first, all search operations seeking incriminating data require informed consent of suspects to volunteer information, lest investigators attract privacy breach claims protected by the right to remain silent and the freedom from trespass.[170]

167 5 of 2018.
168 Secs 36(4)(a) & (b) PTA (n 30).
169 S Kiplagat 'Court frees State to roll out Maisha Namba' *Business Daily* 23 February 2024, https://www.businessdailyafrica.com/bd/economy/court-frees-state-to-roll-out-maisha-namba-4534574 (accessed 16 March 2024).
170 Art 49(1)(b) Constitution of Kenya.

Second, even if the police do not secretly plant incriminating evidence to frame a suspect, by denying the court a chance to limit the intrusive scope of intended searches, they are deemed to harm the suspect's inherent dignity. Hence, to enshrine the presumption of innocence, 'Miranda warnings' inform arrested persons of their right against self-incrimination.[171] Where reasonable suspicion of a non-cognisable offence exists, save for special circumstances recorded by police, investigators need court warrants to authorise targeted surveillance.[172] Consequently, in *Philomena Mbete Mwilu v Director of Public Prosecutions & 3 Others*[173] Kenya's Constitutional Court excluded incriminating evidence of allegedly fraudulent bank deposits as they were discovered in Imperial Bank accounts extraneous to those that the warrants targeted. Violating privacy by unwarranted searches was detrimental to the administration of justice.

Regarding balancing, although wire taps and eavesdropping on conversations endanger privacy, nevertheless, the Constitution's article 31 privacy protection is derogable. If requesting a data subject's consent may alert them to conceal incriminating evidence or commit a crime, then *ex parte* limited warrants may be sought to intrude into an unwitting targeted suspect's private space, seeking specified data.[174] Therefore recognising the Ethics and Anti-Corruption Commission's police powers during gathering operations, including tracing assets in bank accounts, the Supreme Court exonerated EACC from issuing notice on intended targets prior to investigations.[175]

8 Conclusion

While section 36 of NISA limitedly authorises courts to permit covert investigation, monitoring or interference with the privacy of persons suspected of committing offences threatening national security, section 36 of PTA specifically authorises courts to order the interception of communications of persons reasonably suspected of terrorism-related offences. To counter potential overreaching, such as the decision handed down in the Court's blanket *Mobile Telephones* appeal, there is no reason why Parliament may not enact similar provisions to PTA to facilitate specific wiretapping while covertly investigating other transnational and organised crimes. Serious transnational crimes and the fear of these not only harm mental and physical health, but even human security and well-being which are key components of individual development.

171 Art 49(1)(a) Constitution of Kenya; see also *Miranda v Arizona* 384 US 436 (1966).
172 Secs 118 CPC (n 24) and 57 & 60 National Police Service Act 11A of 2011.
173 *Mwilu v DPP; Stanley Muluvi Kiima (Interested Party); International Commission of Jurists Kenya Chapter (Amicus Curiae)* [2019] eKLR para 349 per Omondi, Ngugi & Tuiyott JJ (as they then were); See also Constitution of Kenya (n 43) art 50(4).
174 J Wangui 'EACC has powers to secretly probe suspect's bank account, apex court rules Friday' 7 October 2022, https://nation.africa/kenya/news/eacc-has-powers-to-secretly-probe-suspect-s-bank-account-apex-court-rules-3977434 (accessed 23 January 2024).
175 *Ethics and Anti-Corruption Commission & Another v Prof Tom Ojienda* Supreme Court 30 of 2019; see also sec 180 Evidence Act (Chapter 80 Laws of Kenya).

Organised crimes also retard economic growth, distort political representation and degrade national values. In the national interest, to benefit from parallel intercept communication, legislative provisions may therefore aid senior police officers to effectively counter specific individuals suspected of piracy, poaching, counterfeiting, and of trafficking in narcotics, illegal firearms, humans or organs and even regarding corruption. This is because in their planning, preparation and perpetration, modern organised criminals invariably deploy digital technology. Africa is awash with these sophisticated devices facilitating serious vices. Consequently, it would be advantageous for criminal justice laws and policies to equip law enforcement officials with commensurate covert powers to detect the electronic and audio footprints of serious organised crimes. Catastrophic social harms accruing from organised criminal acts justify enhancing forensic tools for their detection and proof. The key limitation of the Court of Appeal's *Mobile Telephones* verdict is that it fails to require spies to demonstrate reasonable suspicion to justify obtaining of inferences from sensitive group data. It condones generalised surveillance. Conversely, requiring limited communication intercept warrants shields sensitive individuals and groups that may otherwise be inclined to 'chill' or avoid using digital spaces. Thus, promoting personal and social growth requires limiting surveillance through judiciously authorising specific intercepts to breach privacy only of those individuals who may be reasonably suspected of posing security threats. Complexly, the rise of big data compounds the challenges facing investigators of transnational organised crimes. Increasingly, sophisticated perpetrators tend to conceal themselves behind technological smokescreens in countries with which Kenya has no mutual legal assistance arrangement. While it is harder for the police to identify anonymous individuals whose communications are targeted for interceptions, they are able to infer group criminality by using big data analytics. Privacy concerns boundary management along spatial and informational aspects. In limited circumstances, where there are justifying security requirements, the judicious authorisation of targeted warrants counter-balances the harm occasioned on intercepting of digital information.

Finally, by the end of 2023, the 'Maisha Namba' database substituting the failed 'Huduma Namba' project is projected to enhance Kenya's documentation of human certificates and identity cards to enhance the management of the state's public services. The ease of identifying individuals through irises and fingerprints would dispense with the need to carry physical identity cards. However, its critics not only decry privacy erosion. They also lament possible discrimination in the recording of statistics. Beyond enacting legislation, to allay eavesdropping fears, there is a need to install firewalls, enforce regulatory compliance and punish violators. The Worldcoin company's recent processing of personal data, apparently brazenly, flouted the DPA's section 25 data protection principle compelling assurances by data processors to ensure that personal data is processed in accordance with the data subject's privacy rights. It also omitted to undertake a section 31 DPIA though public participation. A pending court case shall interpret big data analytics to determine its impact on collecting biodata

of hundreds of thousands of Kenyans for unknown purposes. Broad respect for privacy embraces the valuable role it plays in enhancing intellect, choice and personal growth. In liberal democracies, only reasonable suspicion of individual or group participation in serious crime or insecurity warrants limited state surveillance on their activities. Future research could therefore assess the security of big data technological bases, whether in private cryptosales and digital trade or outsourced by the government, including for deployment in electronic voting.

African Journal on Privacy & Data Protection

To cite: T Davis & W Trott 'The regulation of artificial intelligence through data protection laws: Insights from South Africa' (2024) 1
African Journal on Privacy & Data Protection 207-219
https://doi.org/10.29053/ajpdp.v1i1.0010

The regulation of artificial intelligence through data protection laws: Insights from South Africa

*Tara Davis**
Senior Associate Attorney, Power & Associates, Johannesburg, South Africa

*Wendy Trott***
Senior Associate Researcher, ALT Advisory, Johannesburg, South Africa

Abstract:

The use of artificial intelligence (AI) has amplified the privacy concerns of big data in the digital era. AI systems collect personal information through covert and complex ways that may undermine consent. Data used in these systems persists indefinitely and is constantly repurposed beyond the original purposes for which consent was obtained. The ability of AI to make inferences raises the prospect of processing information about data subjects that never consented in the first place, and AI's reliance on big data incentivises behaviour that undermines the data minimisation principle common to most data protection frameworks. Despite these risks, the regulation of AI is woefully lacking in the African context. The only binding domestic legislation in most African states that addresses any form of automated decision making is data protection laws. This article explores the effectiveness of data protection laws in mitigating the risks posed by AI using the example of South Africa.

* BA (RU), LLB (UCT), LLM (Wits); tara.davis@powerlaw.africa
** BA (UGA), MA (Sciences Po Paris); wendy.trott@altadvisory.africa

Key words: data protection; artificial intelligence; privacy; data minimisation; consent

1 Introduction

Artificial intelligence (AI) has permeated the everyday activities of our lives. Beyond its use in search engines and navigation, it also creates images of Pope Francis in a puffer jacket,[1] wins art competitions,[2] and writes and directs movies.[3] It is here, and it is here to stay. It brings with it enormous potential and a significant number of risks – particularly those related to data protection and the right to privacy.

This article explores the regulation of AI through data protection legislation. First, it unpacks AI and the privacy risks it poses. Second, it examines the ways in which AI is regulated in Africa, highlighting that, at present, the only domestic legislation in most African countries that addresses AI in any way is data protection legislation. Third, it analyses the effectiveness of data protection laws in regulating AI by using South Africa's data protection law as a case study. It concludes that although data protection laws currently are the primary method through which AI is regulated on the continent, they are insufficient to protect against the extensive privacy risks posed by AI.

2 What is artificial intelligence?

There is no globally-accepted definition of AI,[4] but it is broadly accepted that AI refers to the implementation of human-like intelligence by a machine.[5] Defining AI is a challenging exercise precisely because 'intelligence' exists on a spectrum: A calculator is intelligent in that it is capable of reliably computing outcomes. The commonly-accepted difference between a calculator and AI is that the latter has intelligence on a multi-dimensional spectrum: It has scale, speed, a

1 '"It's not even real?' Social media stunned by AI image of Pope Francis wearing a stylish puffer coat' *Independent* 26 March 2023, https://www.independent.co.uk/life-style/fashion/pope-francis-ai-image-puffer-b2308159.html (accessed 30 October 2023).

2 'Art made by AI wins fine arts competition' *Impakter* 13 September 2022, https://impakter.com/art-made-by-ai-wins-fine-arts-competition/ (accessed 30 October 2023).

3 No Film School 'This film was written and directed by AI – Here's the how and what you can learn' 23 December 2022, https://nofilmschool.com/2022/12/filmmakers-use-ai-write-and-direct-short-film-and-it-actually-makes-some-sense (accessed 23 March 2023).

4 P Stone and others 'Artificial intelligence and life in 2030: One hundred year study on artificial intelligence: Report of the 2015-2016 Study Panel' September 2016 Stanford University, http://ai100.stanford.edu/2016-report (accessed 30 October 2023).

5 The society for the study of artificial intelligence and simulation of behaviour 'What is AI?' 5 September 2013, https://aisb.org.uk/what-is-ai/ (accessed 23 March 2023). Professor John McCarthy, who first coined the term, defined it as 'the science and engineering of making intelligent machines'. Standford University Human-Centred Artificial Intelligence 'Artificial intelligence definitions' (2020), https://hai.stanford.edu/sites/default/files/2020-09/AI-Definitions-HAI.pdf (accessed 30 October 2023).

degree of autonomy, and generality.[6] AI is an umbrella term – often vaguely and confusingly used – that can refer to a relatively wide range of technologies that fall somewhere on this spectrum, ranging from content-classification algorithms and speech recognition software to ChatGPT and self-directing robots.

Certain AI applications can mimic specific human-like attributes, such as language processing or speech recognition. AI uses certain techniques, one of which is machine learning, which uses training data to teach systems to accurately solve a specified problem in a given domain.[7] These techniques are currently used to develop and implement artificial *narrow* intelligence and are evident in current uses of AI.[8] For example, AI-powered content classification programmes may take an image as *input* and produce as an *output* the probability that the image is that of South African President Cyril Ramaphosa. The AI programme is accordingly trained on large data sets – in this case, images that are either of President Cyril Ramaphosa or not. As noted by the Information Commissioner's Office of the United Kingdom,[9] '[t]his may not sound very different from standard methods of data analysis. But the difference is that AI programmes don't linearly analyse data in the way they were originally programmed. Instead, they learn from the data in order to respond intelligently to new data and adapt their outputs accordingly.'

Large data sets, therefore, are crucial for the development of AI programmes – their training requires a large amount of varied data.[10] AI programmes exist in a 'complex, interdependent, global data ecosystem'[11] in which AI-produced outputs can also be used as new input data for further AI training models.[12] AI has also been enabled by the development of 'big data technologies' such as improved computing storage capabilities and super-fast processing machines in recent years,[13] facilitating the collection and processing of previously inconceivably large quantities of data. It is for this reason that AI is closely associated with 'big data,'[14] a term used to describe 'the explosion of available information'.[15]

6 Stone and others (n 4).
7 Media Monitoring Africa 'The implications of artificial intelligence on information rights' November 2021, https://mediamonitoringafrica.org/wordpress22/wp-content/uploads/2022/10/Media-Monitoring-Africa-Discussion-Document-on-AI.pdf (accessed 28 March 2023).
8 At present, artificial general intelligence, a term that refers to a machine's ability to complete several tasks at a level at least equivalent to that of a human across multiple domains, has not yet been developed.
9 Information Commissioner's Office 'Big data, artificial intelligence, machine learning and data protection' v2.2. 8, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (accessed 23 March 2023).
10 L Mitrou 'Data protection, artificial intelligence and cognitive services: Is the General Data Protection Regulation (GDPR) "artificial intelligence-proof"?' *SSRN* 31 December 2018 7, https://ssrn.com/abstract=3386914 (accessed 28 March 2023).
11 L McGregor, D Murray & V Ng 'International human rights law as a framework for algorithmic accountability' (2019) *British Institute of International and Comparative Law* 310.
12 As above.
13 R Kune and others 'The anatomy of big data computing' (2015) 46 *Journal of Software: Practice and Experience* 79-105.
14 Information Commissioner's Office (n 9) 6.
15 J Fan, F Han & H Liu 'Challenges with big data analysis' (2014) 1 *National Science Review* 293.

3 Privacy risks posed by artificial intelligence

Because of the necessarily close relationship between AI and big data, its use raises serious privacy concerns on several vectors.[16] The right to privacy is enshrined in article 12 of the Universal Declaration of Human Rights (Universal Declaration) and article 17 of the International Covenant on Civil and Political Rights (ICCPR), and it is recognised as an enabler of other fundamental human rights. The right to privacy has undergone significant change in the digital era as new technologies have developed. Inherent in the modern conception of the right is the recognition that 'individuals should determine what information about themselves is made public[17] and control how that information is collected and used'.[18] This implies informed consent and knowledge of what one's data is used for.

AI forms the backbone of search algorithms, recommendation engines and facial recognition systems. Many of these systems collect extensive personal information, such as email addresses, pregnancy status, or pictures of one's face, and use it to influence behaviour by, for example, recommending a particular movie or an ante-natal vitamin[19] or influencing students' behaviour or attendance at school.[20] In some instances, AI is used to scrape text content on the internet to fuel generative AI chatbots.[21] Scraping is just one of several new and increasingly-covert methods used to collect users' information online.[22] This raises serious questions about whether meaningful consent is or can be obtained in such cases. Data used in AI systems also persists indefinitely and is constantly repurposed for use beyond its original purposes, undermining a data subject's ability to understand how and why it is used.[23]

In addition to data that is collected directly from data subjects, AI is also capable of analysing large quantities of observed, derived and inferred data, and, as a result of the latter, making inferences and predictions far beyond human

16 S Dilmaghani and others 'Privacy and security of big data in AI systems: A research and standards perspective' (2019) *IEEE*.
17 D Milo & P Stein *A practical guide to media law* (2013) 51.
18 J Neethling 'Die reg of privaatheid' LLD thesis, UNISA, 1976 358.
19 C Duhigg 'How companies learn your secrets' *New York Times Magazine* 16 February 2012, https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=1&hp (accessed 20 November 2023).
20 J Karoub 'U-M study finds facial recognition technology in schools presents many problems, recommends ban' 10 August 2020, https://news.umich.edu/u-m-study-finds-facial-recognition-technology-in-schools-presents-many-problems-recommends-ban/ (accessed 20 November 2023); M Andrejevic & N Selwyn 'Facial recognition technology in schools: Critical questions and concerns' (2019) 45 *Learning, Media and Technology* 115.
21 'ChatGPT is a data privacy nightmare. If you've ever posted online, you ought to be concerned' *The Conversation* 10 February 2023, https://theconversation.com/chatgpt-is-a-data-privacy-nightmare-if-youve-ever-posted-online-you-ought-to-be-concerned-199283 (accessed 28 March 2023).
22 Mitrou (n 10) 22.
23 Mitrou (n 10) 20.

capacity and traditional data protection conceptions.[24] Provided with only a small amount of data, AI can generate or infer new data about existing data subjects as well as those that did not originally provide their data.[25] The ability to withdraw consent for such use is challenging after data has been incorporated into an AI system.[26] The use of large quantities of data to feed AI systems can also make real anonymisation impossible or enable the re-identification of anonymised data,[27] with the ability to infer the identity of data subjects that have not provided consent for such based on a combination of data points.

Advanced data analysis and AI tools are used to act on these inferences by influencing people's behaviour in some benign ways – such as making movie recommendations – and those that are more concerning – such as electoral decisions and automated disinformation.[28] Is there consent when data subjects have little understanding of what inferences are being developed about them and how they are being targeted or influenced based on those inferences?

More generally, AI has incentivised a culture of collection in which the maximum amount of data is sought to meet the needs of 'big data', as discussed above.[29] For example, AI is used to feed digital advertising algorithms with micro-targeted data collected on a mass scale, monetising the most personal and private aspects of a user's life such as personality traits, cell phone history and emotional states.[30] This raises questions about the violation of the data minimisation principle that is a widely-accepted element of the right to privacy in the digital age.[31]

As pointed out by the United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinions and Expression:[32]

> Because AI systems work by exploiting existing datasets and creating new ones, the ability of individuals to know, understand and exercise control over how their data are used is deprived of practical meaning in the context of AI. Once data are

24 Media Monitoring Africa 'The implications of artificial intelligence on information rights' November 2021, https://mediamonitoringafrica.org/wordpress22/wp-content/uploads/2022/10/Media-Monitoring-Africa-Discussion-Document-on-AI.pdf (accessed 28 March 2023).

25 B Lepri, N Oliver & A Pentland 'Ethical machines: The human-centric use of artificial intelligence' (2021) 24 *iScience* 102249.

26 E Fosch Villaronga, P Kieseberg & T Li 'Humans forget, machines remember: Artificial intelligence and the right to be forgotten' (2018) 34 *Computer Law and Security Review* 304-313.

27 K Manheim & L Kaplan 'Artificial intelligence: Risks to privacy and democracy' (2018) 21 *Yale Journal of Law and Technology* 106.

28 N Bontridder & Y Poullet 'The role of artificial intelligence in disinformation' (2021) *Data and Policy* 1.

29 Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, United Nations General Assembly, A/73/348 29 August 2018 11.

30 Manheim & Kaplan (n 27).

31 AC Raul, F Blythe & S Porath Rockwell 'Privacy by design and data minimisation' (2022) *Global Data Review* 13.

32 Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (n 29).

repurposed in an AI system, they lose their original context, increasing the risk that data about individuals will become inaccurate or out of date and depriving individuals of the ability to rectify or delete the data.

Once fed into AI systems, data can be reused and repurposed, and take on a life of their own. It is unclear how and to what extent the quality and correctness of personal information that has been used in such a system can be maintained over the longer term. Biased, poor-quality, or outdated underlying data can also affect AI's outputs. This may compromise other rights such as equality and freedom from discrimination when AI[33] is used to make consequential decisions about a person such as their likelihood of recidivism.[34] The significant data disparities that exist, particularly in Africa, mean that unrepresentative or inaccurate training data is a major concern for data subjects' consent and control over the use of their information.[35]

As the deployment of AI rapidly progresses across the African continent,[36] it becomes increasingly necessary and urgent to evaluate the steps that are being taken to regulate these technologies and guard against the privacy risks they pose.

4 Artificial intelligence governance in Africa

Research reveals that disturbingly few measures have been implemented to govern the deployment of AI in Africa.[37] Regulation may mean a range of interventions, from behavioural control and self-regulation through to legislation.[38] There have been several developments in Africa in recent years of normative self-regulation programmes and principles by civil society, academics and international and continental organisations. For example, in 2021 the African Commission on Human and Peoples' Rights (African Commission) adopted Resolution 473 on the need to undertake a study on human and peoples' rights and artificial intelligence (AI), robotics, and other new and emerging technologies in Africa.[39]

33 European Union Agency for Fundamental Rights 'Bias in algorithms – Artificial intelligence and discrimination' 8 December 2022, https://fra.europa.eu/en/publication/2022/bias-algorithm (accessed 28 March 2023).

34 M Farayola and others 'Fairness of AI in predicting the risk of recidivism: Review and phase mapping of AI fairness techniques' (2023) ARES 2023: The 18th International Conference on Availability, Reliability and Security.

35 P Gehl Sampath 'Governing artificial intelligence in an age of inequality,' (2021) 12 *Global Policy Special Issue: Digital Technology and the Political Determinants of Health Inequities* 21-31.

36 A Gwagwa & E Kraemer-Mbul 'Artificial intelligence (AI) deployments in Africa: Benefits, challenges and policy dimensions' (2020) 25 *African Journal of Information and Communication* 1-28.

37 ALT Advisory 'AI governance in Africa' September 2022, www.ai.altadvisory.africa (accessed 28 March 2023). The research reviewed six indicators of AI governance, which included dedicated AI legislation, rights regarding automated decision-making in data protection legislation, national AI strategies; draft policies or white/green papers on AI; the establishment of an expert commission or similar entity; and whether AI is a priority in the country's current National Development Plan.

38 S Chesterman *We, the robots?* (2021) 3-4.

39 African Commission on Human and Peoples' Rights Resolution on the need to undertake a study on human and peoples' rights and artificial intelligence (AI), robotics and other new and

However, both these non-binding guidelines and existing African regional human rights law frameworks are ill-equipped to deal with the complexity of AI and its potentially significant consequences for individual and collective privacy rights.[40] For present purposes, we therefore focus on the need for domestic legislation due to its uniquely-binding and authoritative nature in the domestic context.

Out of the 55 African countries,[41] only one – Mauritius – has legislation that meaningfully deals with AI, although it only applies to the financial sector.[42] Only seven countries have a national AI strategy[43] and only Tunisia has a draft policy on AI.[44] There has been a rise in the establishment of expert bodies – 13 countries have established some form of taskforce to deal with AI concerns[45] – and the publication of AI strategies that flag the need to address the ethical and rights implications of AI through improved legislation.[46] However, the dearth of regulation through binding dedicated legislation on AI has meant that data protection laws have become the most common default form of regulation in Africa at the domestic level.

---

emerging technologies in Africa ACHPR/Res. 473 (EXT.OS/ XXXI) 2021 2021, https://achpr.au.int/en/adopted-resolutions/473-resolution-need-undertake-study-human-and-peoples-rights-and-art (accessed 31 October 2023).

40 Z Xaba 'Governing artificial intelligence under the African human rights system: Drawing lessons from international best practices' LLM dissertation, University of Pretoria, 2021; L Lane 'Clarifying human rights standards through artificial intelligence initiatives' (2022) 71 *ICLQ: British Institute of International and Comparative Law* 915-944.

41 Our research focused on the 55 current African Union member states.

42 In 2021 the Financial Services Commission issued rules related to robotic and artificial intelligence enabled services, under the Financial Services (Robotic and Artificial Intelligence Enabled Advisory Services) Rules. The rules regulate licensing procedures for entities that provide investment and portfolio management services enabled by artificial intelligence. One of the compliance requirements for licensees – under sec 10(1) – is to ensure that adequate policies and controls are in place to ensure that algorithms perform as intended and for the design, testing, and monitoring of algorithms. Sec 13 also provides for the submission of independent evaluation reports on algorithms and software systems, and sec 12 requires licensees to retain details of all algorithms and software used.

43 These are Algeria, Benin, Egypt, Morocco, Sierra Leone, Mauritius and Uganda. Note that an AI strategy is defined differently to an AI policy or white paper.

44 'Tunisie: Quatre ministères se mobilisent en faveur de l'Intelligence artificielle' *Challenges* 21 February 2022, https://www.webmanagercenter.com/2022/02/21/480963/tunisie-quatre-ministeres-se-mobilisent-en-faveur-de-lintelligence-artificielle/ (accessed 29 March 2023).

45 These include Algeria, Benin, Egypt, Ethiopia, Kenya, Mauritius, Morocco, Namibia, Nigeria, Rwanda, Sierra Leon, South Africa, Tunisia and Uganda.

46 Eg, the Mauritius National AI Strategy calls for government to 'ensure a conducive environment [for AI] through a robust and yet friendly regulatory, ethics and data protection environment', touches on the complexity of enabling accountability in the use of AI, calls for the establishment of a permanent committee on ethics to maintain dialogue and formulate proposals, posits the possible need for amendments to data protection legislation to address AI, and highlights the need for a 'clear, explicit, and transparent code of ethics' on AI. See Mauritius Artificial Intelligence Strategy November 2018 4 & 67, https://ncb.govmu.org/ncb/strategicplans/MauritiusAIStrategy2018.pdf (accessed 22 February 2023). Egypt's National AI Strategy proposes the creation of a dedicated track for the National Council for Artificial Intelligence on AI ethics that includes a mandate to develop appropriate legislation and regulations and publish guidelines for the Responsible and Ethical Development of AI. See National Council for Artificial Intelligence 'Egypt Artificial Intelligence Strategy' 23 & 38, https://mcit.gov.eg/Upcont/Documents/Publications_672021000_Egypt-National-AI-Strategy-English.pdf (accessed 22 February 2023).

As of March 2023, 38 African countries have data protection laws either in force or in draft form.[47] Data protection laws provide a natural foundation for AI regulatory frameworks.[48] This is so because AI applications often *process* personal information as defined in most data protection laws. They do so in two ways:[49]

> [Personal information] can be used in the creation of datasets which are subsequently used to train AI machine-learning systems to construct algorithmic models; and conversely, such algorithmic models can be applied to datasets of personal information in order to draw inferences pertaining to particular individuals.

In light of this, several countries explicitly include automated processing within the scope of application of their data protection laws. Where they apply, automated processing of personal information must consequently comply with the requirements for lawful processing as specified in data protection laws. Notably, this would include compliance with common requirements such as data minimisation, consent and purpose specification. While AI can in many ways be implemented in compliance with these principles, on the surface, some of these principles seem at odds with the operation of AI.[50]

For example, purpose specification becomes challenging in a system that is designed to constantly iterate on inputs to generate new findings and which learns over time to complete new tasks. As such, this also raises concerns about consent. What is meaningful consent in a context in which uses are still undefined at the point of collection and when inferences are made to generate new data? AI, therefore, has fundamentally reshaped the scope of key data protection principles, including access and control.[51]

Thirty of the draft or in-force data protection laws in Africa contain a provision explicitly dealing with automated decision making as it relates to personal information.[52] Many of these closely resemble one another. In general, they create a right for data subjects not to be subject to certain types of automated decisions. These are either legal decisions intended to evaluate aspects of a person's personality, and/or decisions with other legal effects based solely on

47 ALT Advisory 'Data protection Africa', https://dataprotection.africa/ (accessed 20 March 2023).

48 K Crawford and others 'AI Now 2019 Report' December 2019 *AI Now Institute*, https://ainowinstitute.org/AI_Now_2019_Report.html (accessed 24 March 2023).

49 P Bhagattjee, A Govuza & L Sebanz 'Regulating artificial intelligence from a data protection perspective – Lessons from the EU' *Without Prejudice* December 2020, https://www.withoutprejudice.co.za/free/article/7172/view (accessed 28 March 2023).

50 European Parliament 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' European Parliamentary Research Service June 2020 5, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (accessed 27 March 2023).

51 Research ICT Africa 'AI in Africa: Regional data protection and privacy policy' Policy Brief 3 December 2019 4, https://researchictafrica.net/wp/wp-content/uploads/2020/11/RANITP2019-3-DataProtection.pdf (accessed 24 March 2023).

52 Algeria, Angola, Benin, Botswana, Burkina Faso, Cabo Verde, Republic of Congo, Côte d'Ivoire, Eswatini, Gabon, Ghana, Guinea, Kenya, Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, Rwanda, São Tomé and Príncipe, Senegal, South Africa, Togolese Republic, Tunisia, Uganda, Zambia and Zimbabwe.

automated data processing intended to profile a person or evaluate aspects of their personality or behaviour.

Some laws go further than this. Botswana's Act 32 and Morocco's Law 09-08 mandate data controllers to notify the regulator before carrying out automated processing with personal information,[53] and others address the principle of 'explainability'.[54]

Benin's Law 2009-09 arguably goes the furthest. It stipulates that automated processing that is likely to exclude persons from the benefit of a right, service or contract or that includes assessments of people's social difficulties requires prior approval from the data protection authority.[55] It also requires responsible parties to notify data subjects that automated decision making has occurred, and to provide information regarding its underlying logic, significance and anticipated consequences.[56] It further provides for a public list of automated processing procedures in use.[57]

Although regulating AI through domestic legislation is a difficult task, some of the leading jurisdictions, such as the United States and Europe, have begun to coalesce around the importance of attempting to do so alongside a series of norms that should govern such efforts.[58] Africa is falling behind in these efforts.

5 South Africa's data protection law and artificial intelligence

The Protection of Personal Information Act 4 of 2013 (POPIA), South Africa's data protection law, contains several data protection principles that are common among other African states' laws.[59] These include, for example, the data subject's consent; the lawfulness of processing; and data minimisation, among others.

In light of the potential tension between data protection principles and the operation of AI, we assess whether South Africa's data protection law, by way of example, provides sufficient safeguards against the privacy-related risks posed by AI by assessing three specific issues, namely, inferred personal information, de-identification, and automated decision making.

53 Botswana Act 32 art 34; Morocco Law 09-08 art 14.
54 Eg, Cabo Verde's Law 133/V/2001 art 12(1)(c) provides that data subjects have the right to know the logic involved in any automatic processing of data concerning them; art 23 of Madagascar's Law 2014-038 on the Protection of Personal Information provides that data subjects have the right to receive information that enables them to know and contest the logic underlying any automatic processing that is used to make a decision about them that produces legal effects; and secs 23(2)(e); 34(2)(a); 37(2)(h) and 38 of the Mauritius Data Protection Act 2017 provide various rights related to automated processing.
55 Sec 407.
56 Secs 415, 416 & 437.
57 Sec 439.
58 Chesterman (n 38) 9.
59 I Ademuyiwa & A Adeniran 'Assessing data protection and privacy in Africa' (2020) *Assessing Digitalisation and Data Governance Issues in Africa* 4-6.

In this regard, it is notable that POPIA defines automated means as 'any equipment capable of operating automatically in response to instructions given for the purpose of processing information'.[60] POPIA explicitly includes the processing of personal information by automated means within its scope of application.[61] The two typical ways in which AI processes personal information – to develop datasets to train AI systems and to analyse and interpret the datasets – constitute 'processing' under POPIA. Processing is defined to mean 'any operation or activity or any set of operations, whether or not by automatic means, concerning personal information', and the definition notes a list of activities that includes 'collection', 'collation', 'use' and 'merging'.[62] Accordingly, the processing of personal information by AI systems should, in certain circumstances, comply with the provisions of POPIA. However, POPIA is silent on several unique challenges posed by AI, as discussed below, making its application clumsy and uncertain in many ways.

5.1 Inferred personal information

As discussed, AI models can be applied to personal information to infer new information about a data subject.[63] For example, a data subject's online shopping history may be analysed to infer their gender. This is new information – but does it constitute new, distinct personal information for the purposes of POPIA? This question has obvious implications for how the information may be lawfully processed. It also raises practical questions about a data subject's control of their information – how can a data subject exercise meaningful control over personal information of which they are unaware? Further, the inference by AI is only a probable one. This implies that it will be wrong in a set number of instances, depending on the error rate, which may undermine the principles of data quality. POPIA is silent on the status of such inferred information, and accordingly it is unclear how it should be treated.

5.2 De-identification

POPIA does not apply to information that has been de-identified.[64] However, AI and the proliferation of data have made it much easier to re-identify anonymised data by linking it with, or drawing probable inferences based on additional data.[65]

60 Sec 3(4) POPIA.
61 Sec 3(1) POPIA.
62 Sec 1 POPIA.
63 European Parliament 'The impact of the General Data Protection Regulation (GDPR) on artificial intelligence' *European Parliamentary Research Service* June 2020 50, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (accessed 27 March 2023).
64 Sec 6(1)(b) POPIA.
65 European Parliament (n 63).

POPIA goes some way towards accounting for this through the definition of de-identification, which requires the deletion of information that 'can be used or manipulated by a *reasonably foreseeable* method to identify the data subject'; or 'can be linked by a *reasonably foreseeable* method to other information that identifies the data subject'.[66] However, POPIA is silent on the threshold for these requirements. A responsible party may not itself have the technological capacity or methods to re-identify such data, but a third party might. Once shared, it may be re-identified, with or without the knowledge of the responsible party, with serious consequences for the rights of the data subject. Accountability in such instances would also be challenging, raising questions with regard to both the responsible party and the party that ultimately implemented the re-identification. Further, it is not clear whether the mere existence of AI's capacity to re-identify data makes it *reasonably foreseeable* that any and all de-identified data could theoretically be re-identified. POPIA currently does not address the challenges that AI poses to de-identified information, making its definition and application uncertain.

5.3 Automated decision making

Section 71 of POPIA is the only provision that explicitly deals with processing conducted by AI. This provision provides:[67]

> (1) Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her, or it, or which affects him, her, or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

Positively, the provision aims to mitigate the risks associated with profiling by AI. However, its wording is broad and unclear and, to date, South Africa's Information Regulator has neither released guidelines on its application, nor have any codes of conduct been published.[68] It accordingly is unclear what types of decisions would be considered to affect a data subject to a *substantial degree*, what the meaning of a *profile* is, and what the threshold for *solely* requires. For example, it is unclear whether a decision would be compliant if a human reviewed and confirmed a decision after it had been made by automated means.

66 Sec 1 POPIA, as included in the definition of 'de-identify'.
67 The right is provided for in sec 5(g) and expanded upon in sec 71 of POPIA.
68 In terms of *GG* 44459, https://inforegulator.org.za/wp-content/uploads/2020/07/20210416-gg44459gen209-POPIA-CoC-CBA.pdf and *GG* 44690, codes of conduct have been compiled for the Banking Association South Africa and the credit Bureau, but they have not been published.

In addition, the provision is narrowly circumscribed in sub-section 2, which provides that the provisions do not apply in certain circumstances relating to the conclusion of contracts and where a code of conduct has been developed.

The potential risks to a data subject's rights are further exacerbated by the lack of notification provisions. POPIA does not place an obligation on the decision maker to notify a data subject that they have been subjected to a decision that was based solely on automated decision making.[69] This oversight renders the right ineffective – without knowing it has occurred, a data subject will be unable to exercise or protect their right. This is particularly so in light of recent research[70] that found that existing mechanisms in data protection law – the right to access information[71] – proved ineffective when trying to ascertain how a data subject's personal information was being used for automated processing. The research found that some of the largest companies are unable to meaningfully respond to data subjects' requests to understand whether and how their personal information is used in automated processing and whether this is in line with the provisions of POPIA.

These examples demonstrate that some of the challenges posed by AI have not been effectively resolved in South Africa's data protection law. Arguably, such findings would likely also apply to the data protection laws of other African countries that contain comparable provisions.

6 Conclusion

Data protection laws can provide some mitigation against the risks posed by AI. By incorporating AI within their scope, a degree of compliance with minimal data protection standards is ensured. However, certain data protection measures are undermined by a lack of consideration for the unique attributes of AI – particularly new and complex ways of collecting data, the creation of inferred data, and the ability to re-identify data. Further analysis is necessary to examine the possible incongruence between AI and certain data protection principles – especifically data minimisation, purpose specification, and consent – as they are embodied in many data protection laws across the African continent.

It is clear that African states must urgently take meaningful steps to address the governance lacuna in which AI is rapidly developing and which threatens a wide array of internationally and domestically-recognised human rights,

69 G Katzav 'Has POPIA adequately prepared people to exercise their right not to be subject to automated decision-making?' (2022) *De Rebus*, https://www.derebus.org.za/has-popia-adequately-prepared-people-to-exercise-their-right-not-to-be-subject-to-automated-decision-making/ (accessed 27 March 2023).

70 ALT Advisory 'Failure to access' *ALT AI*, https://ai.altadvisory.africa/wp-content/uploads/Failure-to-Access-AI-transparency-in-South-Africa-2022.pdf (accessed 24 March 2023).

71 Provided for in sec 5(g) of POPIA.

most notably the right to privacy. Further research into interpretations given in other jurisdictions, such as the European Union (EU) under the General Data Protection Regulation, to some common concepts that remain undefined in South African law, such as a *profile* and *processing based solely on automated means,* would assist to provide greater legal clarity. More research is needed to meaningfully regulate AI and provide effective protection for privacy and other rights.

African Journal on Privacy & Data Protection

To cite: E Salami & I Nwankwo 'Regulating the privacy aspects of artificial intelligence systems in Nigeria: A primer' (2024) 1
African Journal on Privacy & Data Protection 220-247
https://doi.org/10.29053/ajpdp.v1i1.0011

Regulating the privacy aspects of artificial intelligence systems in Nigeria: A primer

*Emmanuel Salami**
Researcher, Faculty of Law, University of Lapland, Rovaniemi, Finland

*Iheanyi Nwankwo***
Research Associate, Institute for Legal Informatics, Leibniz Universität, Hannover, Germany

Abstract:

As with the rest of the world, artificial intelligence (AI) systems, including chatbots, medical AI systems, agricultural optimisation systems, and so forth, are witnessing increased deployment in Nigeria. AI presents novel opportunities for innovation and tackling inefficiencies in several sectors of the Nigerian economy. However, its proliferation may result in a plethora of concerns if not developed and deployed within the bounds of law and ethics. Such concerns include the compromise of human rights, reinforcement of unlawful discrimination, compression of the privacy sphere of individuals, violation of the right to data protection, and so forth. This article focuses on the threats and vulnerabilities inherent in the development and deployment of AI as it impacts the right to privacy and data protection in Nigeria. These concerns have necessitated AI regulations and policies across the globe, and there is a consensus that AI systems must ensure respect for human rights and the rule of law, generally, and the right to privacy and data protection, specifically. Given data's prominent role in the AI life cycle, it is not surprising that privacy and data protection laws provide a fertile

* LLB (Lagos), LLM (Hannover), PhD (Lapland); me@emmanuelsalami.com
** LLB (Nig), BL, PhD, CC; nwankwo@iri.uni-hannover.de

basis for assessing AI systems' compliance regimes. At the time of writing, Nigeria is drafting a national AI policy and has only recently passed a data protection legislation. However, Nigeria's AI regulatory strategy has not been adequately examined from the perspective of privacy and data protection law. Therefore, this article seeks to fill this gap by exploring the tension between data protection law and the AI data processing life cycle in the Nigerian context. First, it reviews Nigeria's AI strategy and existing data protection framework and argues that they might be inadequate to address the challenges posed by AI. The article then recommends measures for balancing privacy and AI innovations in Nigeria with global best practices. Finally, it concludes that a robust and principled approach to AI regulation is essential to safeguarding privacy and data protection rights in Nigeria.

Key words: artificial intelligence; data protection; privacy; Nigeria; AI policy

1 Introduction

Global discussions about artificial intelligence (AI) have gained momentum with recent advancements in generative pre-trained transformers (GPTs)' natural language processing.[1] Although AI systems have been deployed in several other sectors, including health care, banking and policing, the impressive output of AI chatbots continues to gain traction. Indeed, there have been success stories around AI systems: More efficient industrial operation management, production cost reduction, and timely solving of complex tasks are some examples.[2] There are also prospects that AI can help in realising global sustainable development goals,[3] and many other use cases keep evolving as AI matures in several fields.

However, AI systems are not infallible; they also pose some risks that some technology experts have acknowledged and even called for a pause in AI development until a set of protocols are agreed upon.[4] For instance, there is evidence of bias reflected in these systems, resulting in discrimination and other (related) human rights violations.[5] Given its capabilities, bad actors can use AI systems to increase surveillance, infringe on the right to privacy, or violate the

1 OpenAI 'GPT-4' 14 March 2023, https://openai.com/research/gpt-4 (accessed 30 March 2023); OpenAI 'Planning for AGI and beyond' 24 February 2023, https://openai.com/blog/planning-for-agi-and-beyond?utm_source=substack&utm_medium=email (accessed 30 March 2023). See also B Gates 'The age of AI has begun' 21 March 2023, https://www.gatesnotes.com/The-Age-of-AI-Has-Begun (accessed 30 March 2023).

2 J Jeong 'Introduction of the first AI impact assessment and future tasks: South Korea discussion' (2022) 11 *Laws* 73.

3 ITU 'United Nations activities on artificial intelligence (AI)' 2021, https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2021-PDF-E.pdf (accessed 30 March 2023).

4 See Future of Life Institute 'Pause giant AI experiments: An open letter', https://futureoflife.org/open-letter/pause-giant-ai-experiments/?utm_source=substack&utm_medium=email (accessed 5 April 2023).

5 FRA 'Bias algorithms – Artificial intelligence and discrimination' 2022, http://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf (accessed 23 March 2023).

rights of vulnerable or minority groups, among other socio-economic impacts.[6] Furthermore, AI development and deployment techniques can impact data protection and ethical principles such as transparency, data minimisation, purpose limitation, accountability, fairness, and so forth.[7]

These concerns are significant, and several regulatory approaches are being devised by international, regional and national authorities to tackle them. For example, the United Nations (UN) and some UN specialised agencies, such as the United Nations Educational, Scientific and Cultural Organisation (UNESCO), have addressed AI-related issues from various perspectives, including human rights and ethics.[8] In his 2021 human rights report, the UN Human Rights Commissioner called for urgent action by states to safeguard human rights in the era of AI. According to him, '[t]he operation of AI systems can facilitate and deepen privacy intrusions and other interference with rights in a variety of ways'.[9] Similarly, the Organisation for Economic Cooperation and Development (OECD) adopted some recommendations on AI that include principles for responsible stewardship of trustworthy AI.[10]

In Europe, the European Union (EU) and the Council of Europe (CoE) have undertaken several initiatives and reforms covering various aspects of AI regulation. The EU, for example, has proposed an AI Act that adopts a risk-based approach to AI regulation.[11] An AI Liability Directive has also been proposed by the European Commission (EC), which aims to make it easier for victims injured by AI-related products or services to bring civil liability claims.[12] These proposals have been followed up with reform to the EU's product liability regime. This reform brings onto the radar emerging technologies, including AI. It will ensure that after product deployment, the factors for consideration when assessing whether a product is defective will include machine learning.[13] Furthermore, the EU High-Level Expert Group on Artificial Intelligence (AI HLEG) has

6 The Alan Turing Institute 'Human rights, democracy, and the rule of law assurance framework for AI systems: A proposal prepared for the Council of Europe's ad hoc committee on artificial intelligence', https://rm.coe.int/huderaf-coe-final-1-2752-6741-5300-v-1/1680a3f688 (accessed 5 April 2023).

7 Jeong (n 2); FRA 'Getting the future right – Artificial intelligence and fundamental rights' 14 December 2020, https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights (accessed 23 March 2023).

8 UNESCO 'Recommendation on the ethics of artificial intelligence' 23 November 2021, https://unesdoc.unesco.org/ark:/48223/pf0000381137 (accessed 23 March 2023).

9 United Nations Human Rights Commission 'Right to privacy in the digital age' 1 October 2021 A/HRC/48/31.

10 OECD 'Recommendations of the Council on artificial intelligence' 22 May 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (accessed 12 February 2023).

11 Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts COM (2021) 206 final.

12 Proposal for a directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM (2022) 496 final.

13 Proposal for a directive of the European Parliament and of the Council on liability for defective products COM (2022) 495 final.

published an Assessment List for Trustworthy Artificial Intelligence to help developers assess the trust level of their AI systems.[14]

The CoE, for its part, is working on AI issues that span several themes.[15] It has issued several recommendations, guidelines and reports, including a recommendation on the human rights impacts of algorithmic systems[16] and guidelines on AI and data protection.[17] In addition, the CoE is spearheading efforts to develop a convention on AI.[18] If this succeeds, it will be the first of such a treaty. It would establish certain fundamental principles, rules and rights to ensure that the design and deployment of AI systems respect human rights, the functioning of democracy and the observance of the rule of law.

In Africa, the African Union (AU) and some African sub-regional groups have started paying attention to AI.[19] For example, the African Union High-Level Panel on Emerging Technologies (APET) has held consultative expert meetings on AI and recommended developing a continental AI strategy for Africa.[20] As a follow-up, a draft of an AU-AI Continental Strategy for Africa is being finalised to be submitted to the AU member states for review and validation, after which a continentally-adopted version will be launched at the beginning of 2024 at the AU Africa Heads of State and Government summit.[21] Recently, the African Commission on Human and Peoples' Rights (African Commission) commenced a focal point study and expert consultation on the impact of AI, robotics and other new and emerging technologies on African human and peoples' rights.[22]

14 High-Level Expert Group on AI (AI HLEG) 'Assessment list for trustworthy artificial intelligence (ALTAI) for self-assessment' 17 July 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68342 (accessed 12 February 2023).

15 Council of Europe's work in progress https://www.coe.int/en/web/artificial-intelligence/work-in-progress#01EN (accessed 28 March 2023).

16 Council of Europe 'Recommendation CM/Rec (2020) 1 of the Committee of Ministers to member states on the human rights impacts of algorithmic systems' 8 April 2020, https://search.coe.int/cm/pages/result_details.aspx?objectid=09000016809e1154 (accessed 28 March 2023).

17 Council of Europe 'Guidelines on artificial intelligence and data protection' T-PD (2019) 01.

18 See Council of Europe 'Revised zero draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law' 6 January 2023, https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f (accessed 28 March 2023).

19 Diplo 'Artificial intelligence in Africa: Continental policies and initiatives', https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/ai-africa-continental-policies/ (accessed 5 August 2023).

20 AUDA-NEPAD 'The African Union artificial intelligence continental strategy for Africa' 30 May 2022, https://www.nepad.org/news/african-union-artificial-intelligence-continental-strategy-africa (accessed 5 April 2023).

21 AUDA-NEPAD 'Artificial intelligence is at the core of discussions in Rwanda as the AU high-level panel on emerging technologies convenes experts to draft the AU-AI continental strategy' 29 March 2023, https://www.nepad.org/news/artificial-intelligence-core-of-discussions-rwanda-au-high-level-panel-emerging (accessed 5 April 2023).

22 African Commission 'Press Release: Inception workshop and experts' consultation on the study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa, 8-9 June 2023, Nairobi, Kenya', https://achpr.au.int/en/news/press-releases/2023-06-08/inception-workshop-and-experts-consultation-artificial-intelligence (accessed 8 August 2023).

Given the traction that AI has gathered globally, it is not surprising that several countries have begun addressing AI issues nationally through policies, regulations and strategies.[23] Thus, there seems to be a global consensus that AI must be regulated to ensure that while reaping the enormous benefits of such technology, it is not used to violate human rights or diminish societal values. Nigeria, like several other countries, is in the process of developing a national AI policy.[24] It has already set up a National Centre for Artificial Intelligence and Robotics (NCAIR),[25] and a National AI Volunteer Expert Group tasked with helping the government draft the national AI policy has concluded its work.[26] Furthermore, the National Information Technology Development Agency (NITDA) has begun drafting a Code of Practice for AI to regulate AI tools such as ChatGPT.[27] While Nigeria's efforts at regulating AI are still at an infant stage, there is an expectation that all these efforts will culminate into a holistic framework that will adequately address emerging AI issues.

One aspect of AI development that has attracted regulatory attention is its impact on the right to privacy and data protection of natural persons (data subjects) whose data is processed to train the AI system or who are impacted by AI-based decisions. Undoubtedly, data is the critical raw material for developing and deploying AI systems – data is the input in AI systems' training, testing and operational processes.[28] Where this data relates to an identified or identifiable natural person (directly or indirectly), the privacy of these data subjects becomes crucial. Not surprisingly, this forms a starting point for measuring the compliance of AI systems within most regulatory frameworks.

Although privacy and data protection concerns are present in other information systems and applications, the design and operation of AI systems have distinct aspects that heighten the risks. These include using algorithms to discover hidden patterns; the opacity of the data processing; the tendency to collect excessive data; data repurposing; and the use of new types of data.[29] When critically analysed, these attributes raise questions as to whether AI systems can comply with data protection principles during their life cycle and to what

23 OECD AI observatory database on national AI policies and strategies, https://oecd.ai/en/dashboards/overview (accessed 5 April 2023).

24 'Developing the national artificial intelligence policy in Nigeria' *Premium Times* 12 August 2022, https://www.premiumtimesng.com/opinion/548380-developing-the-national-artificial-intelligence-policy-in-nigeria-by-fom-gyem.html?tztc=1 (accessed 20 March 2023).

25 https://ncair.nitda.gov.ng/?page_id=2584 (accessed 20 March 2023).

26 C Izuogu 'The artificial intelligence policy I envision for Nigeria', https://www.techpolicy.com.ng/the-artificial-intelligence-policy-i-envision-for-nigeria/ (accessed 30 March 2023).

27 E Ojukwu 'NITDA drafting the Nigeria Code of Practice for artificial intelligence tools such as ChatGPT and others', https://www.tekedia.com/nitda-drafting-the-nigeria-code-of-practice-for-artificial-intelligence-tools-such-as-chatgpt-and-others/ (accessed 8 August 2023).

28 International Organisation for Standards ISO/IEC TR 24368:2022 information technology – artificial intelligence – overview of ethical and societal concerns, https://www.iso.org/standard/74296.html (accessed 5 April 2023).

29 ICO 'Big data, artificial intelligence, machine learning and data protection' (ver 2.2 September 2017) 9, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (accessed 12 March 2023).

extent they could be used to exacerbate privacy violations. These concerns are compelling, given the ability of AI systems to discover unknown patterns and capabilities in surveillance, including through advanced facial recognition systems and profiling, among others.[30]

Therefore, it is not unusual for regulatory instruments to provide data subjects affected by AI systems with the agency over their data and accord them rights where privacy infraction occurs. Recent developments, for instance, allow data subjects to request an explanation of automated processes and human intervention to mitigate the risk of using a wholly automated system to process data that can significantly affect the data subjects. This approach is exemplified in the EU's General Data Protection Regulation (GDPR), which accords data subjects the right to information and 'not to be subject to a decision based solely on automated processing, including profiling'.[31]

Given this direction of travel, it is pertinent to look at Nigeria's AI policy and regulatory framework, especially at how these address privacy and data protection concerns in the context of AI systems' development and deployment. This is essential because AI systems are increasingly being deployed in several sectors of the Nigerian economy, including the financial, agriculture, health and education sectors.[32] As such, it is crucial to investigate how ready Nigeria's privacy and data protection regime is to address any concerns that might arise from using AI.

It is well-known that Nigeria's constitutional guarantee of the right to privacy is not detailed and may not have contemplated the complexities of emerging technologies such as AI systems. Thus, there has been a need for a more specific regulatory framework that defines how informational privacy is to be enforced. It was only in 2019 that the Nigerian Data Protection Regulation (NDPR)[33] was issued to regulate personal data processing, incorporating data protection principles and giving certain rights to data subjects. As this article is being drafted, the Nigeria Data Protection Act 2023 (NDPA)[34] was signed into law and would operate alongside the NDPR.[35] Although many observers have heralded these developments, there has been little investigation into how these instruments regulate AI development and deployment in relation to data protection implications.

Therefore, this article explores how these instruments address concerns around personal data processing throughout the AI systems' life cycles – development

30 ISO/IEC TR 24368 (n 28).
31 General Data Protection Regulation of 2016 arts 12, 13, 14 & 22.
32 D Eke and others (eds) *Responsible AI in Africa: Challenges and opportunities* (2023); K Bala and others 'Artificial-intelligence-based models coupled with correspondence analysis visualisation on ART – Cases from Gombe State, Nigeria: A comparative study' (2023) 13 *Life* 715.
33 https://ndpb.gov.ng/Files/NigeriaDataProtectionRegulation.pdf (accessed 12 January 2023).
34 Nigeria Data Protection Act 37 of 2023 A719-758.
35 Nigeria Data Protection Act 37 of 2023 sec 64(2)(f).

and deployment. The aim is to provide a primer on the potential challenges and privacy threats associated with personal data processing during the design and operational phases of AI systems in Nigeria, as well as recommend ways to address the gaps. The article is structured as follows: Part 2 defines artificial intelligence; part 3 gives an overview of Nigeria's privacy and data protection regime; part 4 analyses Nigeria's AI policy; part 5 explores privacy and data protection concerns associated with developing and deploying AI systems in Nigeria; part 6 discusses some salient findings of the articles, while part 7 provides some recommendations and concludes the article.

2 Defining artificial intelligence

As in the case of several other technological concepts, adopting a universal definition of AI has been challenging, especially because various stakeholders approach the concept from different perspectives. Moreover, several technologies exhibit different aspects of human intelligence and perform in an automated manner that falls within the realm of AI technology. Therefore, it is not surprising that no single definition that captures an array of technologies that could be termed AI has been agreed upon.

Several definitions could be cited to show this diversity. For example, the OECD defines an AI system as

> a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (eg with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy.[36]

While this definition attempts to capture several elements of AI, it sacrifices brevity. To forestall this, other entities have adopted a shorter definition. The International Organisation for Standards (ISO), for instance, defines an AI system as 'an engineered system that generates outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives'.[37] Academics have also contributed to the quest to define AI.[38] McCarthy, credited

36 OECD 'OECD AI principles overview', https://oecd.ai/en/ai-principles (accessed 28 February 2023). The revised draft of the proposed EU's AI Act also defines AI in similar terms as 'a system that is designed to operate with elements of autonomy and that, based on machine and/or human-provided data and inputs, infers how to achieve a given set of objectives using machine learning and/or logic- and knowledge-based approaches, and produces system-generated outputs such as content (generative AI systems), predictions, recommendations or decisions, influencing the environments with which the AI system interacts' (n 11) art 3.

37 International Organisation for Standardisation 'ISO/IEC 22989:2022 information technology – artificial intelligence – artificial intelligence concepts and terminology', https://www.iso.org/standard/74296.html (accessed 5 April 2023).

38 Eke and others (n 32).

as the father of AI, defines AI as 'the science and engineering of making intelligent machines, especially intelligent computer programmes, related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable'.[39]

In Nigeria, a few attempts have been made to define AI at a policy level. For example, the NITDA's draft national data strategy defines AI as 'the creation of intelligent objects that work and react like humans to carry out certain tasks meant for intelligent beings without human intervention'.[40] This definition by NITDA is fascinating as it suggests that AI systems do not require human intervention, contrary to the reality of the technology in some cases.[41]

While the above definitions capture several elements of AI, they bolster the fact that stakeholders view AI from diverse perspectives, which makes it challenging to append a single meaning to the concept and calls for perhaps a practical approach to defining AI contextually, given the multifaceted nature and the several technologies (including robotics, automation and machine learning) around AI. This article does not focus on harmonising the various definitions. However, it suggests a contextual approach to the definition of AI to avoid overly complex conceptual definitions that create uncertainty and make it difficult for a lay person to understand. Thus, AI systems could be seen as intelligent systems designed to 'think' and 'act' like humans in various contexts, with varying levels of human intervention.[42] In this sense, AI can be contextualised by the specific task that the system is designed to perform.[43]

39 J McCarthy 'What is AI/AI basics', http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html (accessed 28 February 2023).

40 NITDA 'National data strategy draft' 2022, https://nitda.gov.ng/wp-content/uploads/2022/11/Final-Draft-National-Data-Strategy.pdf (accessed 30 March 2023).

41 There are many instances where AI systems require human input and intervention. See P Samuelson 'AI authorship?' (2020) 63 *Communications of the ACM* 22.

42 Using automated vehicles as a yardstick, the Society of Automobile Engineers classified six levels of human intervention required in automated vehicles. Level 0 comes with no automation at all; levels 1 and 2, the system takes over some of the driving tasks, but the driver is required to continually monitor the system and must take over the driving when necessary; level 3 requires less monitoring of the system by the driver; in level 4 the system is able to drive the car in normal operation and in defined surroundings while the driver can intervene at will; level 5 is the final and fully-automated and autonomous driving stage. See Society of Automobile Engineers 'SAE international releases updated visual chart for its 'levels of driving automation' standard for self-driving vehicles' 11 December 2018, https://www.sae.org/news/press-room/2018/12/sae-internationalreleases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-drivingvehicles (accessed 3 April 2023).

43 Based on their capability to function independently, AI systems can also be classified as Strong AI (also known as Artificial General Intelligence (AGI)) and Weak AI (also known as Narrow AI). Strong AI describes conscious, self-aware, self-teaching, independent and autonomous AI systems that can solve problems independently. Strong AI systems are largely futuristic and remain an academic discourse at the time of writing. On the other hand, weak AI systems focus on performing specific tasks with human intervention. See B Marr 'What is the difference between weak (narrow) and strong (general) artificial intelligence (AI)' 21 July 2021, https://bernardmarr.com/what-is-the-difference-between-weak-narrow-and-strong-general-artificial-intelligence-ai/ (accessed 28 March 2023); Society of Automobile Engineers (n 42). For further reading on the extent of human intervention required at the current level of human intervention, see Samuelson (n 41).

3 Overview of Nigeria's privacy and data protection regime

Nigeria is one of the countries with a constitutional right to privacy. Section 37 of the Constitution provides that '[t]he privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected'. However, as Omotubora rightly noted, this provision only presents 'a general prohibition from interference';[44] the Constitution did not define privacy or give it a clear scope. The expectation, therefore, is that other laws will fill this gap, determining the boundaries of this right and the principles and conditions for any lawful interference with it. Over the years, several laws and subsidiary instruments have been advanced for this purpose. However, until recently, most of these are sector-specific or marginally contain provisions on privacy as incidental to their core objective.[45]

Recently, the Court of Appeal acknowledged that the contours of the right to privacy could be appreciated by looking at the various laws and regulations made in furtherance or limitation thereof and the judicial interpretation of their application in Nigeria.[46] Therefore, any inquiry into Nigeria's privacy law must consider the various instruments that have been advanced to enforce or limit it. Apart from the pronouncement by the Court of Appeal above, the judicial interpretation of this constitutional right has also significantly influenced the development. Where necessary, the courts have examined these other instruments and have notably favoured a broad interpretation of the right to privacy in Nigeria. In *MDPDT v Okonkwo*, for instance, the Supreme Court declared: 'The sum total of the rights of privacy and of freedom of thought, conscience or religion which an individual has, put in a nutshell, is that an individual should be left alone to choose a course for his life, unless a clear and compelling overriding state interest justifies the contrary.'[47] To this end, the Court of Appeal has also pronounced that personal data protection is integral to the right to privacy guaranteed under the Constitution.[48] However, the Court has so far not established principles for personal data protection. Therefore, reliance would be placed on the principles in the secondary laws.

Apart from the judicial influence in this area, several regulatory authorities in Nigeria are reflecting the global trend by adopting data protection requirements

44 A Omotubora 'The NITDA regulations on data protection: A peculiarly Nigerian approach?' 28 June 2019, https://mikedugeri.wordpress.com/2019/06/28/the-nitda-regulations-on-data-protection-a-peculiarly-nigerian-approach/ (accessed 12 February 2022).

45 I Nwankwo 'Information privacy in Nigeria' in A Makulilo (ed) *African data privacy laws* (2016); UV Obi 'Data privacy and data protection law in Nigeria' 14 April 2022, https://www.mondaq.com/nigeria/privacy-protection/1183140/data-privacy-and-data-protection-law-in-nigeria (accessed 12 January 2023).

46 *Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission* Appeal CA/IB/291/2020.

47 *MDPDT v Okonkwo* (2002) AHRLR 159 (NgSC 2001) para 73; *Nwali v EBSIEC* [2014] CA/E/510/2013.

48 *Incorporated Trustees of Digital Rights Lawyers Initiative* (n 46) 23.

in areas where personal data processing is significant, such as banking and telecommunications. These regulators have issued many guidelines and codes of practice that impact data protection within their sector.[49] In 2019 NITDA published a general regulation, the NDPR, as an instrument of general application. NDPR imitated the EU's GDPR in several respects: It contains principles of personal data processing, the obligations of data controllers and processors, accords certain rights to data subjects and muted a few enforcement mechanisms.

However, NDPR has several shortcomings and has been severely criticised,[50] including for its peculiar language and structure and lack of independent supervisory authority. Most importantly, whether NDPR implements section 37 of the Constitution is unclear. Moreover, the courts have refused to enforce its provisions through the fundamental rights enforcement mechanism,[51] suggesting that its legal basis lies in the NITDA Act rather than the Constitution. It is also notable that NITDA has published two other guidelines, namely, the Guidelines for the Management of Personal Data by Public Institutions in Nigeria[52] and the Nigeria Data Protection Regulation 2019: Implementation Framework,[53] which are meant to clarify the provisions of NDPR. Surprisingly, in some respects, these documents have introduced new requirements beyond what NDPR provides, thereby creating uncertainty about their relevance.[54]

Given the shortcomings of NDPR, the NDPA has been welcomed by all stakeholders with the expectation that its implementation will fill the gaps in the system.[55] The Act provides a legal framework for personal data protection and aims, among others, to safeguard the fundamental rights, freedoms and interests of data subjects, as guaranteed by the Constitution.[56] It contains data protection principles, obligations of data controllers and processors, rights of data subjects

49 See the Central Bank of Nigeria Circular to Banks and Non-Bank Financial Institutions Issuance of Consumer Protection Regulations (20 December 2019); CBN's Framework Consumer Protection for Banks and Other Financial Institutions Regulated by CBN (2016); NCC's Consumer Code of Practice Regulation (CCPR) 2007; NCC's Registration of Telephone Subscribers Regulation 2011.

50 Omotubora (n 44). See also A Omotubora 'How (not) to regulate data processing: Assessing Nigeria's Data Protection Regulation 2019 (NDPR)' (2021) 2 *Global Privacy Law Review* 186-199.

51 *Incorporated Trustees of Digital Lawyers Initiative (on behalf of data subjects whose personal data were exposed by the Unity Bank Plc) v Unity Bank Plc* (unreported) Suit FCH/AB/CS/85/2020; *Incorporated Trustees of Digital Lawyers Initiative (on behalf of Daniel John) v National Identity Management Commission* (unreported) Suit FHC/AB/CS/79/2020.

52 NITDA 'Guidelines for the management of personal data by public institutions in Nigeria, 2020', https://ndpb.gov.ng/Files/GuidelinesForImplementationOfNDPRInPublicInstitutions Final11.pdf (accessed 14 January 2023).

53 NITDA 'Nigeria data protection regulation 2019: Implementation framework' March 2021, https://nitda.gov.ng/wp-content/uploads/2021/01/NDPR-Implementation-Framework.pdf (accessed 14 January 2023).

54 Surprisingly, though, in some respects, these documents have introduced new requirements beyond what the NDPR provides. This has resulted in ambiguity and has possibly made the Nigerian data protection framework incomprehensible to lay persons.

55 It is remarkable that there have been several attempts at passing a federal data protection act in Nigeria since 2005. See Nwankwo (n 45).

56 Nigeria Data Protection Act of 2023 sec 1.

and enforcement mechanisms. Notably, the NDPA established the Nigeria Data Protection Commission (NDPC) to oversee its enforcement. The Act did not repeal NDPR; both instruments will operate concurrently.

As further discussed, the data protection principles in these instruments will impact the AI life cycle. For example, the NDPA requires that the processing of personal data must be lawful, meaning that it must be based on any of the permissible grounds listed in the Act, including consent, contract performance, compliance with a legal obligation, for the vital interest of the data subject, public interest task or legitimate interest of the data controller, processor or third party. The processing must also comply with other principles, such as purpose limitation, adequacy, data minimisation, storage limitation, accuracy, data security and duty of care.[57] In the same vein, AI systems must be designed to enable data subjects to enforce their rights, such as rights to information, rectification, erasure, not to be subject to a decision based solely on automated processing of personal data, among others.

In the following analysis, the relevant provisions of the NDPA and NDPR will form the focus of this article to determine their adequacy in regulating the privacy aspects of AI.

4 Artificial intelligence policy in Nigeria

As earlier noted, several AI systems are in use in Nigeria. These AI systems are used by various Nigerian institutions, including banks that deploy AI for anti-money laundering and credit risk assessment systems to ministries, departments and government agencies that use them for multiple services, such as deploying the vehicle identification number (VIN) valuation system by the Nigerian Customs Service.[58] Some of these AI systems are highlighted in Table 1 below:

57 Nigeria Data Protection Act of 2023 sec 24

58 D Olawuni 'Nigerian customs introduce new valuation system for imported vehicles' 14 January 2022, https://dailytrend.com.ng/2022/01/14/nigerian-customs-introduce-new-valuation-system-for-imported-vehicles/ (accessed 20 March 2023).

AI system/AI manufacturer	Function
Renewable Africa 365	This AI system has been developed to identify locations in Nigeria where solar power would be most viable and likely to impact the community positively.[59]
Thetaray[60]	Some Nigerian banks have deployed this AI system to identify suspicious transaction patterns that require further examination.[61]
Airsmat	Airsmat's AI system helps farm owners access information such as suitable crops to farm based on soil composition, crop count on the farm, weed and disease detection, etc.[62]
Ubenwa	This AI system supports the early identification of neurological and respiratory conditions in infants.[63]
Zenvus Smartfarm	This AI-powered precision farming solution uses an intelligent electronic sensor to help farmers optimise crop yields and reduce wastage by analysing soil data and providing real-time crop monitoring.[64]
Kudi.ai	Using natural language commands, this AI-powered chatbot allows users to perform various financial transactions such as bill payments, airtime recharge, and money transfers.[65]

Table 1: Some examples of AI systems in Nigeria[66]

Given the use of AI systems enumerated above and others not mentioned, it is not surprising that AI-related concerns have attracted regulatory attention in Nigeria, including that of NITDA, the government agency that promotes and regulates technology. In the Nigerian government's National Digital Economy Policy and Strategy, AI and machine learning are recognised as emerging technologies that will help boost Nigeria's economy and citizens' well-being and address national challenges.[67] Accordingly, NITDA has spearheaded the

59 'Harnessing AI for renewable energy access in Africa' 27 April 2021, https://ai4good.org/blog/harnessing-ai-for-renewable-energy-access-in-africa/ (accessed 21 March 2023).
60 https://www.thetaray.com/anti-money-laundering/ (accessed 20 March 2023).
61 A Pugh 'Nigerian fintech Arca taps ThetaRay for AI-powered AML solution' 8 September 2023, https://www.fintechfutures.com/2022/09/nigerian-fintech-arca-taps-thetaray-for-ai-powered-aml-solution/ (accessed 23 March 2023).
62 https://airsmat.com/farmmanager (accessed 23 March 2023).
63 https://www.ubenwa.ai/ (accessed 20 March 2023).
64 https://www.zenvus.com/products/smartfarm/ (accessed 20 March 2023).
65 https://techpoint.africa/2017/02/08/kudi-ai-online-payments-nigeria/ (accessed 20 March 2023). See also https://nomba.com/ (accessed 20 March 2023).
66 A perusal of the websites and relevant policies of these AI systems (and their developers) does not expressly reveal the types of data processed by these AI systems.
67 Federal Ministry of Communications and Digital Economy 'Nigerian government's national digital economy policy and strategy 2020-2030' November 2019, https://ndpb.gov.ng/Files/Policy-National_Digital_Economy_Policy_and_Strategy.pdf (accessed 20 March 2023).

establishment of NCAIR[68] and is developing an AI policy for Nigeria.[69] NITDA also established a National AI Volunteer Expert Group tasked with helping draft the national AI policy, which has completed its task.[70] At the time of writing this article, a draft of the AI policy has gone through NITDA's internal review and sent to the Federal Executive Council for approval.[71] Furthermore, NITDA has indicated it is drafting a Code of Practice for AI to regulate the use of AI tools, such as generative AI tools and their impact on privacy, bias, misinformation, deepfake, among other issues.[72] Amidst the risks associated with Large Language Models (LLM) like ChatGPT, NITDA intends that such a code will reflect the peculiar nature of the Nigerian environment to ensure responsible and ethical deployment of AI tools.

While this is ongoing, the Federal Ministry of Communications, Innovations and Digital Economy has hinted at its strategy on AI for Nigeria.[73] A White paper published by the ministry acknowledged that AI has evolved into a multifaceted technology with enormous economic and social potential. As such, the government is poised to adopt a 'co-creation' approach in developing Nigeria's AI strategy for sustainable development, with input from top Al researchers of Nigerian descent globally. The ministry has already started curating a list of leading researchers, in the hope that it will help build innovative technological solutions to solve national problems and create opportunities for citizens.

As of the time of writing, none of these initiatives has resulted in a concrete documented framework allowing a detailed analysis of privacy and data protection aspects around Nigeria's AI policy. In general, stakeholders have advised the regulator to adopt a rights-based approach in developing the AI policy, hoping this will eventually result in thoughtful laws and regulations that mandate responsible and trustworthy AI development and deployment.[74] The themes proposed for the futuristic policy include transparency, human rights, ethics, privacy and data protection, trust and robustness. These are laudable themes, and it is hoped that they will be at the forefront of any future policy to enhance AI advancement in Nigeria. In addition, they will assist in promoting competitiveness and societal respect for human rights and development. Therefore, policy makers must thoroughly evaluate the Nigerian environment,

68 https://ncair.nitda.gov.ng/?page_id=2584 (accessed 20 March 2023).
69 *Premium Times* (n 24).
70 Izuogu (n 26).
71 N Isaac 'FG finalises policy on AI, commends volunteers for contributions' 8 March 2023, https://sciencenigeria.com/fg-finalises-policy-on-ai-commends-volunteers-for-contributions/ (accessed 30 March 2023). Unfortunately, the draft was not publicly available for review at the time of writing in March 2023.
72 Ojukwu (n 27).
73 B Tijani, https://twitter.com/bosuntijani/status/1696113557354549599 (accessed 10 September 2023).
74 J Effoduh 'Towards a rights-respecting artificial intelligence policy for Nigeria' November 2021, https://paradigmhq.org/wp-content/uploads/2021/11/Towards-A-Rights-Respecting-Artificial-Intelligence-Policy-for-Nigeria.pdf?ref=benjamindada-com-modern-tech-media-in-ssa (accessed 30 March 2023).

including existing laws, and provide AI policies to enhance regulatory certainty and guide stakeholders in developing and deploying responsible AI.

5 Privacy and data protection concerns associated with AI systems in Nigeria

As established in the preceding part, the deployment rate of AI systems in Nigeria necessitates legal regulation. This part, therefore, will focus on the privacy and data protection regulatory aspects of AI in Nigeria and primarily considers AI systems in their development and deployment stages. AI's development and deployment stages are coinages of this article that underline critical stages in the AI life cycle. As will be discussed, some of the concerns and implications of AI systems arise in the machine-learning phase well before its launch. Some other concerns and implications arise after deploying the AI system and might be (un)connected to the machine-learning phase. The essence of this classification is to prevent convolution by approaching these privacy and data protection law concerns based on how they might occur. However, it is notable that some unavoidable overlaps may occur in such classification, especially concerning incidental and interrelated matters.

5.1 AI development stage

This is the phase where AI systems are created, potentially from the ideation stage to the actual building, testing and preparation of the AI for deployment. Undoubtedly, data plays an essential role in this phase.[75] Much of the progress achieved lately in AI development stems from the availability of more data for use in the machine-learning phase.[76] However, this stage is critical to AI's output because, with AI systems, the 'garbage in, garbage out' mantra holds ever true. Therefore, the output generated by the AI system is determined by the quality of the training data. To appreciate the criticality of data processing during the development phase and the tensions that may arise from a data protection perspective, some relevant issues will be considered in the context of the NDPR and the NDPA. Although these concerns are multifaceted and complex, the following analysis will primarily revolve around considerations, which include the legal basis for data collection, data quality and data minimisation.

75 J McKendrick 'The data paradox: Artificial intelligence needs data; data needs AI' 7 June 2021, https://www.forbes.com/sites/joemckendrick/2021/06/27/the-data-paradox-artificial-intelligence-needs-data-data-needs-ai/ (accessed 27 March 2023).

76 C Gröger 'There is no AI without data' (2021) 64 *Communications of the ACM* 98.

5.1.1 Legal basis for data collection

Data collection is a foundational phase in the AI development stage. Given its impact on AI's future deployment and output, this phase is critical because once the training or foundational data ingested by AI is tainted, that taint will likely reflect in and/or affect the data output. Where there is no reliance on a legal basis or a defective legal basis is relied upon to collect data for model training, the unlawful nature of the processing activity taints the data. This is particularly relevant when personal data is included in the large volumes of big data used to train AI systems. For instance, as of 2020, AI developer Clearview AI is said to have used about 4 billion pictures to train its facial recognition technology.[77] However, various data protection authorities have since fined Clearview AI for violating data protection principles, including unlawful data collection.[78]

The crux of this issue is that (global) data protection legislation, including the NDPA, requires that any processing of personal data shall be lawful, that is, rely on a legal base while complying with other applicable data processing principles and requirements. Irrespective of whether data used in training an AI model is obtained from open sources, failure to observe these legal requirements infringes the affected data subjects' rights. This is even crucial when data collection techniques, such as web scraping,[79] are analysed within the scope of data protection law.

A perusal of the website (including privacy policies/terms and conditions) of the AI developers/service providers listed in Table 1 does not mention or reveal how their data was collected for model training. However, there is no doubt that large volumes of (personal) data are required and must have been used to train these AI systems, thereby bringing this process within the purview of data protection law and necessitating compliance by all stakeholders. As such, any unlawful data processing at this phase embodies a risk that will likely affect the operational phase of the system and its output. One such risk is a possible suspension of the use of the AI system by supervisory authorities pending clarification of its compliance status, as seen with the Italian data protection authority's suspension of Open AI's ChatGPT and Replika in Italy.[80]

77 T Cushing 'How much data does clearview AI gather on people? The answer (sadly) will not surprise you' 27 March 2020, https://www.techdirt.com/2020/03/27/how-much-data-does-clearview-gather-people-answer-sadly-will-not-surprise-you/ (accessed 27 March 2023).

78 The French, Greek and Italian data protection authorities have variously fined Clearview AI for reasons related to unlawful data collection. See B Toulas 'Clearview gets third €20 million fine for illegal data collection' 21 October 2022, https://www.bleepingcomputer.com/news/security/clearview-ai-gets-third-20-million-fine-for-illegal-data-collection/ (accessed 27 March 2023).

79 Data scraping generally involves the automated extraction of data from the web. See Joint statement on data scraping and the protection of privacy, https://ico.org.uk/media/about-the-ico/documents/4026232/joint-statement-data-scraping-202308.pdf (accessed 27 March 2023).

80 Garante per la protezione dei dati Personali 'Artificial intelligence: Stop to ChatGPT by the Italian SA personal data is collected unlawfully, no age verification system is in place for

An appropriate legal basis for data collection is a critical data protection consideration in all stages of the AI life cycle. NDPR provides, among other things, that personal data shall be lawfully processed based on consent, the performance of a contract, compliance with a legal obligation, the vital interest of the data subject, and public interest.[81] Section 25 of NDPA equally tows this line but includes an additional basis – 'legitimate interests pursued by the data controller or data processor or by a third party to whom the data is disclosed'. Suffice it to say that the Nigerian data protection framework covers personal data collection during AI development, irrespective of whether the data is obtained from open or closed sources.

On the part of the developers of the AI system, concerns around the issue of a legal basis for data collection can arise in two ways: first, when personal data that has not been lawfully collected (for instance, through web scraping devoid of an appropriate and justifiable legal basis) is used during the machine learning process.[82] This would result in unlawful data processing since the system has been developed with unlawfully-obtained data. Assuming that the AI systems identified in Table 1 above have been developed with data collected from Nigeria(ns), it is unclear what legal basis the developers would have relied upon to collect the data, as no evidence of this is publicly available on their website. Second, it is possible for AI systems to process (personal) data in a manner that was not intended at the commencement of the processing activity.[83] In such an event, the initial legal basis for the activity might not suffice again, particularly when considering that the data processing purpose has changed.[84]

5.1.2 Data quality

Another critical concern at the AI development stage is the quality of data used during machine learning. Again, where personal data is involved, the data protection principle of data quality requires that data controllers/processors process data that is accurate and fit for purpose. Therefore, using biased and/or inaccurate data that does not represent the targeted population, whether imported from offline sources or online, to train AI systems violates this principle. For example, biased data that contains the stereotypes existing in offline spaces, when imported into the AI system, can potentially result in the adoption of

children' 31 March 2023, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870847#english (accessed 2 April 2023).

81 Nigeria Data Protection Regulation of 2019 secs 2.1 & 2.2. See also Nigeria Data Protection Act of 2023 sec 25 for a similar provision.

82 The French data protection supervisory authority, CNIL, issued a fine against Clearview AI for similar reasons. See CNIL 'Facial recognition: 20 million euros penalty against clearview AI', https://www.cnil.fr/en/facial-recognition-20-million-euros-penalty-against-clearview-ai (accessed 27 March 2023). For further reading on web scraping, see B Sobel 'A new common law of web scraping' (2020) 25 *Lewis & Clark Law Review*, https://law.lclark.edu/live/files/31605-7-sobel-article-251pdf (accessed 27 March 2023).

83 D Bloch 'Machine learning: models and algorithms' 27 May 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3307566 (accessed 27 March 2023).

84 Nigeria Data Protection Regulation 2019 sec 2.1 (1)(a) for further grounds of data processing.

unlawful discriminatory practices by AI systems. A practical manifestation of this possibility has been observed in the United States, where the use of AI for (predictive) policing, including crime prediction, neighbourhood surveillance, vehicle plate number identification, facial recognition, and so forth, is fraught with discrimination imported from data sources with which the AI was trained.[85] During machine learning, a backlog of biased data is typically fed into the AI system, thereby systematically creating a bias in its outcome.[86] More specifically, reliance on racially-imbalanced data that reflects the racial sentiments of a human police officer will only train the AI to act like any other racially-biased human police officer.[87] Based on this use case, one can conclude that the importation of biased or inaccurate data at the data collection stage of AI can result in biased and other adverse outcomes.

As such, an argument can be made for a breach of the principle of data quality in these cases. The data quality principle can be gleaned from NDPR and NDPA through the data accuracy principle. NDPR provides that personal data shall be 'adequate, accurate and without prejudice to the dignity of the human person'.[88] NDPA is more detailed and provides that personal data shall be 'accurate, complete, not misleading and, where necessary, kept up to date regarding the purposes for which the personal data was collected or is further processed.'[89] Arguably, this provision seeks to guarantee data quality and adequacy throughout the life cycle of the processing operation. It even covers further processing (referred to in this article as data repurposing). Thus, AI systems developed in Nigeria with poor quality and biased data will potentially infringe on the law. Therefore, it is necessary that AI developers thoroughly check the quality of the data they use in training their models to be compliant with the relevant data protection law in Nigeria.

5.1.3 Data minimisation

The possible collection of more data than is necessary for the processing activity is another concern that is likely in the use of AI. According to the data minimisation principle, data controllers and processors are limited to collecting and processing only the minimum amount of personal data necessary to fulfil a specific purpose. NDPR reflects this principle in its requirement that personal data processed shall be 'adequate, accurate and without prejudice to the dignity of the human person'.[90] However, a more robust provision of the data minimisation principle has been included in NDPA, which provides that a data controller or data

85 AG Ferguson *The rise of big data policing: Surveillance, race, and the future of law enforcement* (2017) 93.
86 As above.
87 As above.
88 See Nigeria Data Protection Regulation of 2019 sec 2.1(1)(b).
89 Nigeria Data Protection Act of 2023 sec 24(1)(e).
90 Nigeria Data Protection Regulation of 2019 sec 2.1(1)(b).

processor shall ensure that personal data is 'adequate, relevant and limited to the minimum necessary for the purposes for which the personal data was collected or further processed'.[91]

Traditionally, large volumes of data are required to train AI systems, including LLM, such as ChatGPT. For example, GPT-3 is reported to have 175 billion parameters and was trained on 570 gigabytes of text.[92] A related concern of excessive data collection is when AI systems capture data independently, especially those that use cameras to scan the environment or automatic speech recognition (ASR)[93] and speech-to-text software. There is the possibility to capture more data than necessary because, in most cases, these data-capturing Internet of Things (IoT) attached to AI systems will capture various data categories in the environment, whether needed or not. These examples run contrary to the data minimisation principle highlighted above.

In sum, while the concerns discussed in this part are not an exhaustive representation of the concerns associated with data protection during AI system development, they have been highlighted to show the tension between standard practices in AI development and relevant data protection principles in Nigeria. More importantly, these concerns may still be prevalent or overlap with others discussed next within the deployment context.

5.2 AI deployment stage

The deployment phase in the AI life cycle is when AI products and services are launched subject to their practical use cases. This phase is not devoid of possible data protection concerns. In the absence of proper planning and preparation, the potential consequences of the AI deployment stage can come as a surprise to AI developers and data controllers/processors. Although several concerns can arise at this stage, the following discussion focuses on transparency, data security, purpose limitation and automated decision issues.

5.2.1 Transparency

Although highlighted here, transparency requirements cut across both the development and deployment phases of the AI life cycle. For example, during data collection, the transparency principle requires providing data subjects with

91 Nigeria Data Protection Act of 2023 sec 25(1)(c).

92 A Tamkin & D Ganguli 'How large language models will transform science, society, and AI' 5 February 2021, https://hai.stanford.edu/news/how-large-language-models-will-transform-science-society-and-ai (accessed 27 March 2023).

93 ASR breaks down speech (either live or recorded) into segments, which are then analysed by the algorithm using natural language processing. For further reading, see D Yu & L Deng *Automatic speech recognition: A deep learning approach* (2014) 1-7.

information about the life cycle of the data processing activity.[94] The AI data deployment stage can also be fraught with transparency concerns. For example, AI systems can be developed with a level of complexity that might make it challenging to explain its functionality. This 'black-box' design means that AI systems may lack the transparency required for data subjects to understand how their data is processed, and decisions arrived at using the system.

In addition, the 'expectation of privacy' principle, handed down by the European Court of Human Rights (ECHR) and now a critical part of privacy law jurisprudence, can also be impacted by the transparency principle.[95] Without transparent information, data subjects will be deprived of their right to be aware of and anticipate the consequences of relevant data processing activities concerning them.[96] This can result in the erosion of trust and the limiting of accountability.

NDPR does not have a unique transparency principle. Rather, it subsumes this principle under the data subject's right to be provided with 'any information relating to processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language.'[97] NDPR further provides that data subjects are to be provided with transparent information before the commencement of the processing activity.[98] A more detailed provision is reflected in NDPA. Section 24(1)(a) of NDPA contains the fairness, lawfulness and transparency principles. The transparency principle requires that relevant information relating to the data processing should be clearly communicated to the data subjects. This principle generally applies to three central areas: providing information to data subjects related to the processing, including the risks and safeguards associated with the processing; how data controllers communicate with data subjects about their rights; and how they facilitate the exercise of these rights.[99]

To further bolster this principle, section 27 of NDPA lists the nature of the information to be provided to the data subject, including the 'existence

94 For further reading, see L Naudts and others 'Meaningful transparency through data rights: A multidimensional analysis' in E Kosta, R Leenes & I Kamara (eds) *Research handbook on EU data protection* (2021), https://ssrn.com/abstract=3949750 (accessed 2 April 2023).

95 This principle pertains to whether the data subject had reasonable expectations of privacy that justify or render an intrusion into their privacy (un)lawful. The origin of this principle is traceable to the jurisprudence of United States privacy law. See P Winn 'Katz and the origins of the "reasonable expectation of privacy" test' (2008) 40 *McGeorge Law Review*, https://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=1204&context=mlr (accessed 2 April 2023). The principle crept into European law around 1997 when it was applied by the ECHR in the *Halford* case. See T Gomez-Arostegui 'Defining private life under the European Convention on Human Rights by referring to reasonable expectations' (2005) 35 *California Western International Law Journal,* 2.

96 *Barbulescu v Romania* (12 January 2016) Application 61496/08. See also Information Commissioner's Office 'Big data, artificial intelligence, machine learning and data protection' 2017, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf paras 39-43 (accessed 2 April 2023).

97 Nigeria Data Protection Regulation of 2019 sec 3.1.

98 Nigeria Data Protection Regulation of 2019 sec 3.1(7); Nigeria Data Protection Act of 2023 sec 28.

99 See UN Right to Privacy Note by the Secretary-General (20 July 2022) A/77/196.

of automated decision-making, profiling, the significance and envisaged consequences of such processing for the data subject, and the right to object to, and challenge such processing'.[100] However, owing to its black-box design and the possibility of AI systems capturing data without the knowledge of the data subject, this may be problematic to achieve. An example of this can be found in AI systems that deploy sensors and cameras for data collection by capturing human faces.[101] In such cases, providing transparent information to data subjects might prove challenging because of the automated, spontaneous and large-scale nature of the data collection.

5.2.2 Data security

Multiple computer networking systems are necessary for AI to function correctly, necessitating considering the security of data being processed by these systems.[102] This is coupled with the large-scale multi-jurisdictional data transfers and IoT attached as components to some AI systems, all requiring varying levels of data security to protect (personal) data. The data security principle requires data controllers and processors to adopt technical and organisational measures to secure both data and systems used to process data to ensure confidentiality, integrity, and availability of personal data. AI systems can suffer glitches that raise significant data protection concerns without adequate security measures.[103]

Section 2.6 of NDPR provides, among other things, that anyone involved in data processing shall develop security measures to protect data, including protecting systems from hackers, setting up firewalls, access control, data encryption, and so forth. Similarly, NDPA includes a data security principle[104] and explicitly requires data controllers and processors to implement appropriate technical and organisational measures towards the security, integrity and confidentiality of personal data under their control.[105] Factors such as the amount and sensitivity of the personal data, the nature, degree and likelihood of harm to data subjects that could result from data breaches, the extent of the processing,

100 Nigeria Data Protection Act of 2023 sec 27(1)(g).
101 These data types are referred to as observed data that are recorded automatically, eg, CCTV cameras, cookies, etc. See Information Commissioner's Office (n 96) 12.
102 Note that data security issues can also arise during the development stage of AI, especially in relation to the processing of data for machine learning.
103 At the time of writing this article, it was reported that the famous AI system Chat GPT had suffered a security breach. See E Kovacs 'ChatGPT data breach confirmed as security firm warns of vulnerable component exploitation' 28 March 2023, https://www.securityweek.com/chatgpt-data-breach-confirmed-as-security-firm-warns-of-vulnerable-component-exploitation/ (accessed 27 March 2023). For further readings on the vulnerabilities of AI and how they can result in security breaches, see M Comiter 'Attacking artificial intelligence: AI's security vulnerability and what policymakers can do about it' August 2019, https://www.belfercenter.org/publication/AttackingAI (accessed 27 March 2023).
104 Nigeria Data Protection Act sec 24(1)(f) and sec 24(2). See also sec 39.
105 Nigeria Data Protection Act sec 39.

data retention period, and so forth, must be considered by them in adopting appropriate data security measures.[106]

However, as stated earlier, maintaining an adequate security framework for AI systems can prove arduous because of the multiple parties and various IoT and data transfers, each susceptible to a vulnerability. Some possible causes of data breaches in AI systems include data tampering, model poisoning, insider threats, and so forth.[107] The criticality of data security to AI can be better appreciated when one considers the recent data breach recorded through Chat GPT and the volume of data affected in the process.[108]

5.2.3 Purpose limitation

A further concern at the AI deployment stage pertains to purpose limitation. The purpose limitation principle requires data controllers to only process personal data for a specified purpose. This is to forestall processing personal data as an afterthought and prohibit further processing, in general, unless such processing is compatible with the original purpose, subject to adequate safeguards and compliance with the relevant rules. In contrast, AI systems can, in some cases, generate results not anticipated at the beginning of the processing activity, and this can encourage data repurposing to achieve a new outcome. An example of this could arise when using unsupervised machine-learning techniques, which can potentially cause unanticipated data processing outcomes.[109] It is usually a suitable device for discovering underlying use cases for data. However, it can pose a concern to the purpose limitation principle.

The purpose limitation principle is reflected in NDPR in several ways. Section 2.5(c) of NDPR provides that the privacy policy shall contain the purpose of collecting personal data. NDPR further provides that should the controller intend to further process the personal data for a purpose other than that for which the personal data has been collected, the controller shall provide the data subject before that further processing with information on that other purpose, and with any other relevant additional information.[110] This provision captures the purpose limitation principle and the rules surrounding data repurposing.[111] Similarly,

106 As above. This provision of the NDPA has a stronger language than that of the NDPR, and quite comparable to the language of international legislation such as the General Data Protection Regulation of 2016 art 32.

107 E Nick 'Top 7 data security threats to AI and ML' 7 December 2022, https://www.datasciencecentral.com/category/business-topics/ (accessed 27 March 2023).

108 Kovacs (n 103). Employees have also inadvertently fed confidential information into AI systems. See L Maddisson 'Samsung workers made a major error by using chatGPT' 4 April 2023, https://www.techradar.com/news/samsung-workers-leaked-company-secrets-by-using-chatgp (accessed 27 March 2023).

109 Unsupervised machine learning draws inference(s) from datasets without reference to known or labelled outcomes. See Bloch (n 83).

110 Nigeria Data Protection Regulation of 2019 sec 3.1(7).

111 See a variant provision on the rules of data repurposing in General Data Protection Regulation of 2016 Art 6(4). For further reading on data repurposing, see P Woodall 'The data repurposing

the purpose limitation principle is also captured in NDPA, which provides that personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'. Further processing is permissible for compatible purposes, such as scientific research, subject to appropriate safeguards, among other considerations.[112]

Therefore, should AI systems be used when their purposes cannot be identified at the beginning of the processing activity and/or maintained throughout the AI life cycle, this can infringe upon the purpose limitation principle. It is common practice to use (personal) data provided by AI users to train the said AI through machine learning.[113] This practice will negatively impact the purpose limitation principle, especially in the event of unsupervised learning.

5.2.4 Automated decisions

AI systems are used for automated decision making, impacting natural persons' rights and freedoms.[114] Using AI for automated decision making can result in unintended risks for data subjects,[115] including depriving patients of access to adequate medical treatment.[116] Given its criticality, it is typical for data protection legislation to include safeguards for the protection of the rights of data subjects. For instance, GDPR has accorded data subjects the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them.[117]

Although NDPR does not contain a similar right for data subjects, it provides, among other things, that in the use of automated decision-making tools, 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing' shall be provided to them before data collection.[118] While this is encouraging, NDPA has filled the gap by providing the data subjects with a 'right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning the data subject'.[119] Although there are exemptions to this right, the problem, as earlier identified, is that many AI

challenge: New pressures from data analytics' (2017) 8 *Journal of Data and Information Quality* 3-4.

112 Nigeria Data Protection Act of 2023 sec 24(4).

113 Eg, this is the practice with AI systems such as Chat GPT that use user data for machine learning. See Chat GPT FAQ, para 6, https://help.openai.com/en/articles/6783457-chatgpt-faq (accessed 4 April 2023).

114 This use case can be found when AI is used in making decisions pertaining to credit scoring, credit lending, mortgage applications, healthcare use, etc.

115 B Mittelstadt and others 'The ethics of algorithms: Mapping the debate' (2016) 3 *Big Data and Society* 2.

116 Z Obermeyer and others 'Dissecting racial bias in an algorithm used to manage the health of populations' (2019) 336 *Science* 447-453.

117 General Data Protection Regulation of 2016 art 22.

118 Nigeria Data Protection Regulation of 2019 sec 3.1(7)(l).

119 Nigeria Data Protection Act of 2023 sec 37.

systems have 'black boxes', making it difficult, if not impossible, to understand the logic behind their decisions. This poses a data protection compliance concern.

Notably, NDPA further requires data controllers to implement suitable measures to safeguard the data subject's fundamental rights, freedoms and interests, including the rights to obtain human intervention, express their views and contest automated decisions.[120] This is a welcomed development, considering that AI systems can be fraught with a large margin of error.[121] Such provision forces AI systems to be deployed in a manner that enables data subjects to enforce their rights.

6 Discussion

It can be observed from the preceding parts that Nigeria's AI policy is still being developed, offering little insight into how privacy and data protection concerns identified above could be tackled. It is uncertain at this stage whether the policy will result in a dedicated AI regulatory instrument such as the proposed EU AI Act that is being negotiated. Despite these shortcomings, there is evidence that NDPA and NDPR, key data protection instruments of general application in Nigeria, contain principles and provisions relevant to regulating AI systems' development and deployment. Although these instruments were not focused on AI when adopted, an analysis of their provisions indicates complementarity of how they can regulate data protection issues arising in the use of AI. For example, while NDPR contains neither the right not to be subject to a decision based solely on automated processing nor human intervention regarding such processing, NDPA has complemented this shortfall.[122] Similarly, the transparency principles that is missing in NDPR are now incorporated in NDPA.

One interesting distinction between NDPR and NDPA is that the former provides data subjects with a right to obtain 'meaningful information about the logic involved' in making automated decisions concerning them.[123] Such provision or its variant is absent from NDPA.[124] The right to explainability of automated decision making has undergone various stages of transformation from academic debates[125] to being featured in legislation[126] and pragmatic implementation. Therefore, it is necessary to retain this feature in the data protection framework to align with international standards in data protection law. Thus, the NDPC

120 Nigeria Data Protection Act of 2023 sec 37(3).
121 These errors could stem from various avenues including bias that originates from the developer's bias and the use of biased datasets.
122 Nigeria Data Protection Act of 2023 (n 119) .
123 See Nigeria Data Protection Regulation of 2019 art 3.1(7)(i).
124 See Nigeria Data Protection Act of 2023 sec 27(1)(g).
125 S Wachter and others 'Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation' (2016) *International Data Privacy Law*, https://ssrn.com/abstract=2903469 (accessed 4 April 2023).
126 This provision is featured in the data protection legislations of some African countries. See, eg, South Africa's Protection of Personal Information Act (POPIA) 2013 sec 71(3)(b).

ought to take advantage of the complementarity of both instruments to avoid uncertainty.

Despite this complementarity, stakeholders should look beyond (the principles of) data protection law and take advantage of the global trend towards a holistic, ethical and risk-based approach to AI regulation. One of the benefits of the worldwide attention that AI has received is the enormity of work undertaken concerning AI regulation, which Nigeria can leverage. A notorious example is the report of the EU's AI HLEG, which can serve as a regulatory guide in shaping AI regulation in Nigeria.[127] One key output of the guidelines of the EU AI HLEG is that for AI to be trustworthy, it ought to be robust while complying with legal and ethical principles.[128] The EU's AI HLEG proposes seven key requirements to consider AI trustworthy. These seven key requirements are human agency and oversight; technical robustness and safety; privacy and data governance; transparency; diversity; non-discrimination and fairness; societal and environmental well-being; and accountability.

Beyond the scope of data protection principles, Nigerian authorities could draw inspiration from global best practices in shaping Nigeria's AI policy direction. This will serve two essential purposes. First, it will ensure that AI systems manufactured in Nigeria are marketable to the rest of the world while ensuring privacy compliance that meets minimum global standards. Second, using international standards will help address the challenges identified in this article, particularly in using biased data during AI development. One possible way of tackling this concern is by adopting tools designed for detecting and mitigating bias in algorithms and ensuring that divergent data that pertains to a broad spectrum of people, cultures, issues, history, and so forth, is used to train AI systems deployed in Nigeria.[129] This way, data will represent various members and interests of society more, which will not be prejudiced by the traditional biases that society has become familiar with. Given Nigeria's lack of regulation, international best practices and ethics become essential to achieving this goal.[130] Therefore, it is suggested that stakeholders deploying AI systems must go beyond the letters of the law and consider ethical principles in the AI life cycle.

Similarly, more emphasis should be placed on using privacy-enhancing mechanisms, such as privacy impact assessments (PIAs) and privacy by design (PbD), especially in scenarios of large-scale data processing, such as web scraping,

127 AI HLEG (n 14).
128 As above.
129 Further measures such as process standardisation and AI/data auditing have been proposed to tackle the problem of biased data. See E Salami 'AI, big data and the protection of personal data in medical practice' (2019) 3 *European Pharmaceutical Law Review* 165-175. Furthermore, tools such as IBM's AI Fairness 360 help in examining bias in machine learning. See IBM 'Introducing AI fairness 360', https://www.ibm.com/blogs/research/2018/09/ai-fairness-360/ (accessed 6 April 2023).
130 For further reading on ethical issues in big data processing, see M Kirsten 'Ethical issues in the big data industry' (2015) 14 *MIS Quarterly Executive* 2.

when developing AI systems in Nigeria. The PIA is a risk assessment tool to identify threats against personal data and other assets. It also analyses the threats and potential harms to the data subjects, aiming to implement measures to mitigate the risks.[131] It is 'anticipatory in nature' and ideally carried out before a project begins, before the risk occurs. On the other hand, PbD centres on embedding privacy consideration into the design specifications of technologies that process personal data or could affect privacy in general.[132] Both tools are proactively used for embedding privacy into the design and operation of personal data-processing activities.[133] These mechanisms are obtainable under Nigeria's existing data protection regime and could be critical to implementing the duty of care and accountability required under section 24(3) of NDPA.

The duty of care requirement provides that a data controller or processor owes a duty of care regarding data processing and shall demonstrate accountability with respect to the principles contained in NDPA. By so doing, NDPA creates a duty of care in favour of data subjects for processing their personal data by controllers and processors. The duty of care is a new introduction to the jurisprudence of Nigerian data protection law, though not entirely new to data protection law itself.[134] Scholars have also argued that a connection exists between the duty of care under the law of torts and privacy.[135] The notorious case of *Donoghue v Stevenson* lays the foundation for the duty of care principle, which requires that a person exercises a duty of care to foreseeable persons (the plaintiff) to prevent them from being harmed.[136]

On the other hand, the accountability principle requires that data controllers and processors should be able to demonstrate compliance with the principles of data protection law. While NDPA refers to the duty of care on only one occasion, it references the accountability principle on three occasions, signalling its importance. By adopting PIA and PbD, some of the concerns highlighted in part 5 of this article will be promptly identified in context, and mitigation will be planned early enough before or during the development of the AI system and/or launching it. Among other things, these mechanisms will ensure that data collection processes involve sufficient considerations of privacy compliance and

131 See I Nwankwo 'Towards a transparent and systematic approach to conducting risk assessment under article 35 of the GDPR' Phd thesis, Gottfried Wilhelm Leibniz Universität, 2021, ii, xxiii, 275 S. DOI: https://doi.org/10.15488/11364 (accessed 12 September 2023).

132 L Bygrave 'Hardwiring privacy' University of Oslo Faculty of Law Research Paper 2017-02. See also A Cavoukian 'Privacy by design: The 7 foundational principles' (2009, revised 2011), https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (accessed 31 July 2019).

133 FRA *Handbook on European data protection law* (2018) 183-184. See also L Bygrave 'Data protection by design and by default: Deciphering the EU's legislative requirements' (2017) 4 *Oslo Law Review* 2; A Cavoukian 'Privacy by design: The 7 foundational principles', https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (accessed 30 March 2023).

134 B van Alsenoy 'Liability under EU data protection law: From Directive 95/46 to the General Data Protection Regulation' (2016) 7 JIPITEC 271 para 1.

135 Alsenoy (n 134).

136 (1932) AC 562.

are entrenched throughout the AI system's life cycle. This, in turn, will ensure compliance with the duty of care and accountability principles.

Notably, irrespective of the discussion above, much responsibility still lies in the data protection supervisory authority, AI developers, controllers, processors, and other stakeholders to pursue privacy compliance on a large scale and to imbed such culture in the AI life cycle. For instance, even though there is a provision requiring a justifiable legal basis for personal data processing in the regulatory instruments considered in this article, the evidence suggests that AI developers do not comply with them. Therefore, regulatory intervention through guidelines, audits, robust whistle-blowing, and enforcement actions will be necessary to secure compliance.[137] In other words, mere reliance on the letters of the law would not yield any benefits without regulatory enforcement actions.

The findings of this article reveal that the NDPC is better suited to enforcing the privacy aspects of AI regulation. Section 5 of NDPA has assigned several functions to the Commission, including the power to regulate the deployment of technological measures to enhance personal data protection, investigate violations of data protection law, collaborate with other ministries and agencies, and carry out legal actions, among others. The NDPC can monitor and enforce data protection compliance within the AI sector if effectively utilised. Any aspect not adequately covered by data protection law, such as using biased data in AI, especially in the machine-learning phase, could be tackled in collaboration with other agencies through further regulatory guidance or legal reform. Although the data quality principle might curb the effects of data bias, additional regulatory guidance remains necessary.[138] It is suggested that law makers and ministers should be proactive and critically analyse all aspects of emerging technologies, including AI, in their functions. Although adopting a technology-neutral approach ensures the applicability of laws irrespective of the technology or activity being assessed, sometimes specific legislation is an excellent tool to address pressing needs.

7 Recommendations and conclusion

This article has examined key data protection issues around developing and deploying AI systems in Nigeria. It has highlighted the tensions between AI techniques and data protection principles. For example, AI systems rely heavily on large amounts of data for model training, and data repurposing is common. These features appear antithetical to data protection principles of data minimisation and purpose limitation. Issues around the legal basis for collecting data, data quality, transparency, data security, and automated decision making

137 Web scaping has been found to be a way through which AI developers collect large volumes of (personal) data (n 79).

138 Eg, AI could have an impact on labour rights where it is used as part of the recruitment process, or for measuring employee performance, etc. In such case, the Federal Ministry of Labour and Employment could team up with the NDPA to tackle the issue of AI in this respect.

have also been explored to demonstrate these challenges. Moreover, AI systems can perpetuate and even exacerbate existing biases in the data used to train the models, leading to discriminatory outcomes.

To address these concerns, some actions are needed in several areas, and the following recommendations are suggested towards addressing them:

(1) AI will have vast implications for Nigerian society, requiring a careful understanding of these impacts to integrate this technology safely and effectively. Therefore, the authorities should invest in AI governance research and ensure it has AI experts throughout this process of adopting a national AI policy. It is welcomed that the Federal Ministry of Communications, Innovations and Digital Economy is already thinking in this direction; it further recommended that this approach be augmented with an expert study on the impact of AI on human rights, particularly on privacy, in Nigeria. This will assist regulatory stakeholders in developing a comprehensive AI human rights framework grounded in global best practices. Given that the challenges posed by AI are global, such a framework should consider international standards, including a proactive, principled, and risk-based approach to AI regulation. This will offer a comparative advantage and position Nigeria at a vantage point to export its AI technology and take pride in developing responsible and ethical AI. Ultimately, the success of AI systems in Nigeria will depend on the regulatory ability to address the complex ethical, legal, and social issues that arise in their development and deployment.

(2) Besides developing a framework, enforcing data protection requirements should be at the forefront of Nigeria's data protection regime, particularly regarding AI. This incidentally will impact how AI developers and deployers consider data protection principles and obligations in their business. Enforcement should emphasise data collection processes, particularly in the machine learning phase, to ensure compliance with the legal basis for data processing requirements. The duty of care and accountability principles should also be effectively used during enforcement to interrogate whether the affected actors have taken reasonable standards of care regarding no harm to data subjects.

(3) Nigeria's AI policy should emphasise the use of privacy-enhancing mechanisms such as PIA and PbD as an integral part of the AI life cycle where such system is to be used to process personal data to ensure that data protection principles are enshrined and implemented throughout all AI-related data-processing activities. This will ensure that AI systems are designed to collect only the minimum amount of (personal) data needed for specific purposes and adhere to stated purposes. Furthermore, using industry standards should be strongly encouraged and recommended to AI system developers. These industry standards are essential because AI technical requirements may vary from industry to industry.

(4) Finally, until NDPR and NDPA are harmonised into a single framework, it is recommended that the regulatory stakeholders interpret and read them in a complementary fashion to address the gaps in each of them as they relate

to AI. In this respect, it is recommended that the NDPC critically review NDPR to address any gaps or conflicts with NDPA to avoid uncertainty.[139]

In conclusion, the proliferation of AI and its emergence as a reliable technology cannot be denied. However, it has also been shown that AI systems are fraught with potential privacy and data protection concerns that require all stakeholders' attention at the various stages of the AI life cycle. This article argues that effective privacy regulation of AI systems is crucial for safeguarding human rights, including the right to privacy and data protection. It also acknowledges the complexities and difficulties of regulating AI systems, particularly given the rapid pace of technological change and the potential for unintended consequences. These recommendations will go a long way in addressing these challenges.

139 Such a review may eventually lead to its repeal or update.