2 Data privacy in Africa: Taking stock of its development after two decades

Alex Boniface Makulilo

Abstract

Exactly two decades have lapsed since the first data protection legislation in Africa was enacted (in Cape Verde). This chapter aims to offer a broad overview of the development of data privacy laws and policies in Africa. The theoretical and philosophical underpinnings of data privacy in Africa as well as factors that have influenced this development are considered. The future development of data privacy in Africa is finally projected against that particular background. The chapter is divided into the following parts: Part 1 provides a general overview of data privacy globally. Part 2 covers the African world view on privacy. Part 3 considers determinants of privacy concerns in Africa over the past two decades. Part 4 provides legal and policy frameworks of data privacy in Africa. Part 5 provides a discussion of the patterns and trends of data privacy policies. Part 6 concludes the chapter.

1 Introduction

Privacy is a Western concept. It has evolved over the years. Bennett observes that record keeping on individuals (one of the reasons why data privacy laws partly emerged to regulate) is as old as civilisation itself.[1] The Roman Empire, for example, maintained an extensive system of taxation records on its subjects, who were identified through census taking.[2] However, the modern conception of privacy and data protection may be traced from Warren and Brandeis's seminal article 'The right to

1 CJ Bennett *Regulating privacy: Data protection and public policy in Europe and the United States* (1992) 18.

2 A Roos 'The law of data (privacy) protection: A comparative and theoretical study' LLD thesis, UNISA, 2003 1-2. See also A Roos 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* 402. It is worth noting that the most extreme example of census abuse is Hitler's use of the census to track minorities for extermination during the Nazi regime. See EPIC 'The census and privacy', http://epic.org/privacy/census/ (accessed 10 November 2021). For more discussion about privacy risks associated with population census, see also the famous census judgment of the German Federal Constitutional Court in 1983, Federal Constitutional Court, Judgment of 15 December 1983, 1 BvR 209/83.

privacy', published in the *Harvard Law Review* in 1890.[3] This article indeed is increasingly acknowledged by commentators as the official birth date of the right to privacy in the world.

It is worth noting that in the 1960s and 1970s concrete privacy and data protection regulations emerged in North America and Europe. This is not surprising as the rise of computer technology around that time increased many possibilities with which organisations, both public and private, as well as individuals could process personal information in ways that could interfere with an individual's privacy. The legal response to the rise of computer technology with respect to the protection of an individual's privacy had been to enact data protection legislation.[4] While technological factors occupied the central role in the emergence of data protection laws, there were other factors that operated as catalysts for such an emergence. Bygrave discusses three main catalysts for emergence of data protection laws: first, technological-organisation trends (growth in amount of data stored and their integration; increased sharing of data across organisational boundaries; growth in re-use and re-purposing of data; increased risk of data misapplication; information quality problems; and diminishing role of data subjects in decision-making processes affecting them); second, public fears (fears over threats to privacy and related values and restriction in transfer of personal data and thereby in goods and services); and, third, legal factors (influence of international human rights instruments proclaiming rights to privacy as well as insufficiency of protection of privacy under existing rules).[5] In 2004 Bygrave expanded on this list to include ideological factors as essential in determining privacy levels. Central among these are attitudes to the value of private life, attitudes to the worth of persons as individuals, and sensitivity to human beings' non-economic and emotional needs.[6] Bygrave notes that the concern over privacy tends to be high in societies espousing liberal ideals.[7]

3 SD Warren & LS Brandeis 'The right to privacy' (1890) 4 *Harvard Law Review*.193-195. This work has frequently and traditionally been cited in numerous scholarly writings on the history of the right to privacy.

4 The first data protection law in the world was adopted by the German *Land* of Hesse in October 1970. Then followed Sweden (1973); the United States (1974); Germany (1977); France, Denmark and Austria (1978); Luxemburg (1979); New Zealand (1982); the United Kingdom (1984); Finland (1987); Ireland, Australia, Japan and The Netherlands (1988). Today almost all Western countries have adopted data protection legislation.

5 LA Bygrave *Data protection law: Approaching its rationale, logic and limits* (2002) ch 6.

6 LA Bygrave 'Privacy protection in a global context – A comparative overview' (2004) 47 *Scandinavian Studies in Law* 328.

7 As above.

However, modern privacy and data protection challenges arise mainly from globalisation, technological progress (for instance, big data analytics, cloud technology, internet of things, artificial intelligence (AI)) and seamless cross-border flows of personal data. It is important to note that every region of the world (Europe, America, Asia, Australia, Africa) is experiencing such challenges. Of course, the magnitude and effect of such challenges differ significantly due to a wide range of factors. Generally speaking, the more a particular society is exposed to technology and associated risks to abuse of personal data, the more such society is likely to raise privacy concerns and demands for its regulation. However, this might not well explain the origins of the concept privacy in most African independent constitutions towards the end of the colonial period in Africa. As Makulilo argues, the concept of privacy developed in Africa at the end of the colonial period, particularly as outgoing colonial powers often left behind constitutions providing protections of privacy, among other values, even though this may have been inconsistent with the more collectivist values of those societies at the time.[8] Despite that, the first data protection legislation on the African continent appeared in Cape Verde in 2001. Since then, other African countries have adopted data privacy laws and policies. Until February 2021 about 30 African states out of 55 (see figure 1)[9] had enacted data protection legislation laws that are closely aligned to the first generation of data privacy laws (that is, the OECD Guidelines 1980 and Council of Europe Convention 1981) and second generation of data privacy laws (that is, EU Directive 95/46/EC). Since 2016 new data protection legislation and revision in Africa have largely been aligned to the third generation of data privacy laws, namely, the EU General Data Protection Regulations 2016 (GDPR).[10] It is worth mentioning that the Council of Europe Convention 108+, which is also part of the third

8 AB Makulilo 'The quest for information privacy in Africa' (2018) 8 *Journal of Information Policy* 324-327.

9 Algeria, Angola, Benin, Botswana, Burkina Faso, Cape Verde, Chad, Congo-Brazzaville, Egypt, Equatorial Guinea, Gabon, Ghana, Guinea Conakry, Côte d'Ivoire, Kenya, Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, São Tomé and Príncipe, Senegal, Seychelles, South Africa, Togo, Tunisia and Uganda. As of 2024, about six more countries have enacted data protection law making the total figure to be 36 countries with data protection laws in Africa.

10 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980; the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (CETS 108), 1981; the General Data Protection Regulation 2016/679Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data 2018.

generation of data privacy laws, has slowly started to exert its influence in Africa following the first accession by Mauritius on 4 September 2020.

This chapter offers a broad overview of the development of data privacy laws and policies in Africa. The theoretical and philosophical underpinnings of data privacy in Africa and the factors that have influenced this development are considered. The future development of data privacy in Africa is finally projected against that particular background. The chapter is divided into the following parts: Part one provides a general overview of data privacy globally. Part two covers the African worldview on privacy. Part three considers determinants of privacy concerns in Africa over the past two decades. Part four provides legal and policy frameworks for data privacy in Africa. Part five discusses the patterns and trends of data privacy policies. Part six concludes the chapter.

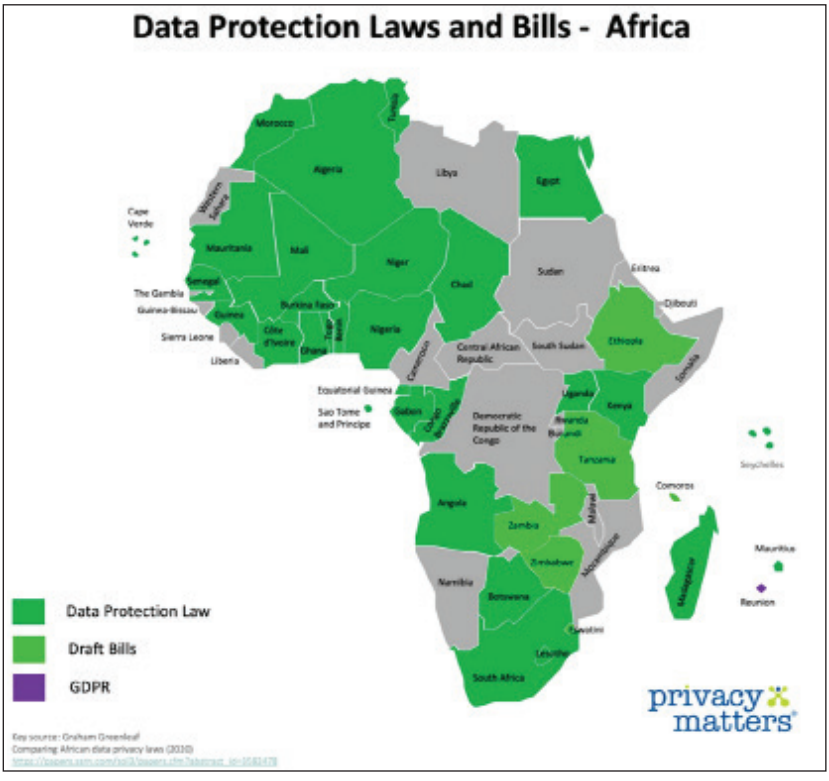

Figure 1 shows the state of data protection laws in Africa as of February 2021.

2 The African world view on privacy

2.1 Privacy notion

In their seminal article 'The right to privacy', renowned legal scholars Warren and Brandeis defined privacy as 'the right to be let alone'. Since this time, different legal and non-legal scholars have conceptualised privacy in different formulations. This chapter does not intend to review debates around the definition of privacy. However, one important point about the various schools of thought is that there yet is no consensus as to the acceptable definition of the notion 'privacy'. Nonetheless, the bottom line of most of the definitions is individualism. That is, privacy is an individual right. Its normative basis is spelt out in international and regional human rights instruments, such as article 12 of the Universal Declaration of Human Rights 1948 (Universal Declaration); article 17 of the International Covenant on Civil and Political Rights 1966 (ICCPR); article 8 of the European Convention on Human Rights 1950 (European Convention); article 17 of the Arab Charter on Human Rights 1994 (Arab Charter); and article 5 of the American Declaration of the Rights and Duties of Man 1948. Surprisingly, the African Charter on Human and Peoples' Rights (African Charter) does not contain a specific provision for the protection of privacy. Because of this, commentators such as Gutwirth argues:

> Insofar as sub-Saharan Africa can be assessed as one whole, privacy stands for little. Notably, the 1981 African Charter on Human and Peoples' Rights does not even mention privacy … The Charter highlights African values and traditions, which give content and meaning to human rights. It centres on community, whether this is family, a group, or a people. The individual cannot fully rely on human rights when faced with the group or state … The status of individual is limited … Individualism is subordinate to the group, reducing the space for privacy. In practice, the dominance of the collective spirit probably even exceeds the boundaries set by the Charter. This is so, even though many African states shortly after obtaining independence partially or fully adopted the legal system of their colonizers, which was based on the individual.[11]

Bygrave similarly argues:

> The liberal affection for privacy is amply demonstrated in the development of legal regimes for privacy protection. These regimes are most comprehensive in Western liberal democracies … By contrast, such regimes are under-developed

11 S Gutwirth *Privacy and the information age* (2002) 24.

> in most African and Asian nations. It is tempting to view this situation as symptomatic of a propensity in African and Asian cultures to place primary value on securing the interests and loyalties of the group at the expense of the individual. However, care must be taken not to paint countries and cultures into static categories. As elaborated in section 5 below, provision for privacy rights is increasingly on the legislative agenda of some African countries. A similar development is occurring in some Asian jurisdictions.[12]

Following some privacy and data protection policy developments in Africa, particularly the adoption of data privacy policies, Bygrave has argued:

> Until recently, African organizations scarcely figured as policy entrepreneurs in the field of data privacy. The situation today is different. Africa is now a home to some of the most prescriptively ambitious data privacy initiatives at the regional and sub-regional levels. The leading initiative comes from the 15 members of ECOWAS. It takes the form of Supplementary Act on Protection of Personal Data within ECOWAS, adopted in 2010.[13]

Despite the development of privacy laws and policies in Africa, there is neither concept nor theory that distinctly deals with privacy in an African cultural context. The specific call for the conceptualisation of privacy in an African context appears only in the works of Bakibinga. As pointed out, Bakibinga holds that an individual in Africa can have privacy and still be part of the community.[14] Building upon this premise, she makes a definitive call specifically on Uganda that privacy has to be defined in a way that is acceptable to the Ugandan society given the emphasis on communalism versus individual rights.[15] She further contends that privacy should not remain an abstract, and one way to start would be to commission studies to obtain perceptions of privacy within Ugandan society.[16]

Currently, the only theory of privacy that has gained prominence in Africa, albeit not in the African cultural context as such, is that of a

12 Bygrave (n 6) 328.

13 LA Bygrave *Data privacy law: An international perspective* (2014) 80.

14 EPIC Alert 'EPIC hosts privacy and public voice conference in Africa' (23 December 2005) Vol 11, No 24, http://www.epic.org/alert/EPIC_Alert_11.24.html (accessed 10 November 2021).

15 EM Bakibinga 'Managing electronic privacy in the telecommunications sub-sector: The Ugandan perspective' 2004 4, http//:thepublicvoic.org/eventscapetown04/bakibinga.doc (accessed 10 November 2021).

16 As above.

renowned professor, Johann Neethling. Neethling's theory of privacy states:

> Privacy is an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he evidences a will for privacy.[17]

The above definition of privacy implies an absence of acquaintance with a person or his personal affairs in his state of seclusion.[18] Accordingly, privacy can only be infringed by the unauthorised acquaintance by an outsider with a person or his personal affairs, which acquaintance can occur in two ways only: first, by intrusion in the private sphere (that is, where an outsider himself becomes acquainted with a person or his personal affairs); and, second, by disclosure or revelation of private facts (that is, where a third party acquaints outsiders with a person of his personal affairs which, although known to that party, remains private).[19] As privacy is closely associated to other personality interests, Neethling has conducted a considerable analysis to distinguish it from such other interests: physical-psychological integrity (including sensory feelings); dignity; identity; autonomy; self-realisation; and patrimonial interests.

Although Neethling's theory of privacy appears to have been postulated in 1976,[20] the theory is not novel. Neethling seems to have relied on a similar theory as propounded by Hyman Gross in 1967.[21] The context in which Gross's conceptualisation of privacy sprang was the US Supreme Court's decision in *Griswold v Connecticut*.[22] In this way it may be argued that Neethling's theory of privacy follows the same pattern of Western individualism. Also important, such theory may be classified as falling under the control theory of privacy concept. This notwithstanding, Neethling's theory of privacy has received wider recognition in literature in Africa. Similarly, Neethling's theory has received the approval of the South African Supreme Court of Appeal in *National Media Ltd v Jooste*.[23]

17 J Neethling and others *Neethling's law of personality* (1996) 36; J Neethling 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 19.

18 J Neethling and others *Neethling's law of personality* (2005) 21.

19 As above.

20 J Neethling 'Die reg op privaatheid' ('The right to privacy') LLD thesis, UNISA, 1976.

21 Gross 'The concept of privacy' (1967) 42 *New York University Law Review* 34-54.

22 381 US 479 [1965].

23 1996 (3) SA 262(A) 271.

3 Determinants of privacy concerns in Africa

Privacy concerns, which means a desire to keep personal information to oneself, are essential in determining the adoption of privacy policies and legislation. In Africa such concerns are influenced by various factors. These may broadly be classified as positive or negative determinants. The former relates to factors that operate to cause individuals to be concerned about their privacy and possibly make claim for its protection. It is less important if those factors themselves are positive or negative in their nature but produce one similar result: causing people to be concerned about and value their privacy. The other class of determinants is the negative determinants in the strict sense. The latter constitutes factors operating as impediments to the growth of privacy attitude. Both sets of determinants are considered below. However, before this examination is undertaken it is imperative to consider their nature.

Privacy determinants in Africa characteristically are either spontaneous or non-spontaneous in operation and in producing their effects. Also, some of them are either localised in a particular country or sub-region while others have region-wide influence. Moreover, one or more determinants may operate simultaneously or otherwise in shaping and reshaping privacy attitudes. Important also to point out is the magnitude of these determinants. Quite often the determinants of privacy concerns produce effects at varying degrees: high and low degree. However, this does not suggest undermining the significance of the latter.

One caveat must be read into the above classification of determinants of privacy concerns. The classification presented here undeniably is neither universal, nor is it exhaustive. Yet, it serves to delineate the current major catalysts of privacy concerns in Africa. These may be the bases for policy and legislative developments. Also considering these determinants as not exhaustive leaves it open for future determinants to arise and shape and reshape privacy attitudes in Africa.

3.1 Positive determinants

Development of data banks: Much of the present-day Information and Communication Technology (ICT) in Africa is a result of importation of technology mainly from Europe, the United States and currently from China. While ICT has been an essential tool for information communication, making Africa part of the famous 'global village', it has at the same time posed a number of risks on individuals' personal information. One of the ways in which personal information apparently

is threatened is African governments' tendencies of creating large data banks for various purposes. The latter has manifested mainly in the form of mandatory registration of SIM cards in which all service providers were and are still required as part of their licensing conditions to register all subscribers using their networks. In most cases, the registration of SIM cards in such countries requires subscribers to furnish a wide range of their personal information. The development of SIM card data banks has sparked public debates over the concern over privacy. Part of the reason is the fact that in many countries, such as Tanzania, Kenya, Nigeria, Ghana and Botswana, to mention but few examples, the mandatory registration of SIM cards proceeded, at least initially, on the basis of administrative directives from the national communication authorities in the respective countries.[24] There was no legislation or regulation in place for the protection of individuals' personal data.

The other important database in Africa includes those on identification systems (ID systems). Identification systems constitute the most common ICT privacy issue currently facing Africa.[25] Such ID systems manifest as national identification cards (national ID cards) leading to the creation of data banks of all nationals in a particular country or passports.[26] Both systems use biometric technology. Concerns over privacy here have arisen from the fact that many of the ID systems, such as those in Rwanda and Mozambique, are developed and operated by foreign companies.[27] While there is no concrete evidence of any misuse of personal data, these concerns have tended to be insufficiently controlled by African governments in order to prevent such companies from transferring information outside their respective jurisdictions or deal with it in an incompatible manner. As a result, companies may misuse personal information at the peril of individuals. Yet, significant concerns come from security issues as well

24 See, eg, AB Makulilo 'Registration of SIM cards in Tanzania: A critical evaluation of the Electronic and Postal Communications Act, 2010' (2011) 17 *Computer and Telecommunications Law Review* 48; M Murungi 'Registration of mobile phone users: Easier said but carefully done' *Kenya Law* (26 July 2009), http://kenyalaw.blogspot.com/2009/07/registration-of-mobile-phone-users.html (accessed 10 November 2021); CE Izuogu 'Data protection and other implications in the ongoing SIM card registration process' (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665 (accessed 10 November 2021); K Anan 'What is my beef against SIM card registration in Ghana?' Independent Civil Advocacy Network, (25 January 2010), http://www.i-can-ghana.com/?p=104 (accessed 10 November 2021); E Sutherland 'The mandatory registration of SIM cards' (2010) 16 *Computer and Telecommunications Law Review* 61.

25 D Banisar 'Linking ICTs: The right to privacy, freedom of expression and access to information' (2010) 16 *East African Journal of Peace and Human Rights* 126.

26 As above.

27 As above.

as reliability of these databases.[28] Rwanda and Kenya (*Huduma Namba* identification system) serve as typical illustrations of misuse of personal information based on ID systems. During the Rwandan genocide of 1994, the national ID cards were used to identify the 'Tutsi' victims.

Apart from SIM cards and national ID data banks, in many African countries there are also centralised voter registration databases (CVRDs). The latter in many cases are computerised databases with biometric information, most invariably fingerprints. Privacy concerns with regard to CVRDs have been raised in three main areas. First, most African countries neither have comprehensive data privacy legislation, nor do such countries have legislation or regulations that authorise the collection of voters' personal information while guaranteeing the protection of privacy.[29] Second, where voter registration involves biometrical registration, individuals' concerns over privacy have been raised high. Third, personal information collected for voting purposes in most cases is shared and re-used for other purposes. This is especially the case in countries where there are no national IDs. In Ghana, apart from voters' ID cards being used by card holders for private transactions, the same cards have been widely recognised and accepted as official identification by various institutions.[30] This is also the case in many other African countries that have not yet adopted national ID card registration systems and sometimes those with national ID systems, such as Tanzania. The privacy issue arising here is that at the time of registration and, hence, the collection of personal data, the respective individuals are not made aware of the disclosure of their personal information to third party institutions or individuals for purposes other than voting. Yet, in defending the practice the electoral commissions, which are the custodians of individuals' personal data, have always argued that since voters voluntarily use voters' registration cards for other transactions they have through that given permission for their personal data to be exchanged between those institutions and voters' roll databases.[31]

Twitter (now X) and Facebook (now Meta) revolutions: The Arab Spring[32] in North Africa has demonstrated the clearest instances of violations of

28 As above.

29 A Evrensel 'Introduction' in A Evrensel (ed) *Voter registration in Africa: A comparative analysis* (2010) 16.

30 Evrensel (n 29) 16-17.

31 As above.

32 The Arab Spring was a series of anti-government protests, uprisings and armed rebellions that spread across much of the Arab world in the early 2010s. See PK Kumaraswamy 'The Arab Spring' (2011) 38 *India International Centre Quarterly* 52

privacy by African governments through the use of modern technologies. First, the Tunisian, Egyptian and Libyan governments used advanced internet filters to block content during the uprisings.[33] In Tunisia the government deployed a far more advanced technology in crackdown through the theft of user names and passwords for Facebook, Twitter and online e-mail accounts such as Gmail and Yahoo![34] This was achieved through the injection of phishing scripts into the content of these pages before being sent to the end user.[35] The identification of users was soon followed by arrests, detentions and harassments of those involved in the creation and dissemination of user-generated content.[36] Second, Twitter and Facebook were highly used as tools of state surveillance by security and state intelligences to identify and locate activists and protestors.[37] Many people participating on Facebook pages were actually government agents or supporters of the regimes, spreading propaganda as well as spying on other Facebook users.[38] Third, the regimes, especially those in Egypt and Libya, also demonstrated their ultimate power over the internet by virtually shutting down access to it[39] or frequently causing interruptions. The Twitter/Facebook revolutions raised awareness to the majority of Africans over the privacy implications in interacting with social networks and other electronic communications variants. The possibilities to be identified when accessing or exchanging information or opinion, for example, and, above all, the potential possibilities of such communications to be intercepted or monitored with advanced technology have raised more privacy concerns.

Fears: Public fears over threats to privacy and related values have made a significant contribution to the emergence and/or existence of data protection laws, at least in Europe.[40] One set of such fears related to increasing transparency, disorientation and disempowerment of data subjects in relation to data controllers.[41] Another set of fears concerned the loss of control over technology. A third set pertained to human dehumanisation of societal processes.[42] In Africa, although it is doubtful

33 Kumaraswamy (n 32) 52.
34 As above.
35 As above.
36 As above.
37 As above.
38 As above.
39 As above.
40 Bygrave (n 5) 107.
41 As above.
42 As above.

whether such fears have had a significant impact in the emergence and/or existence of data protection laws, sufficient fears have been raised regarding privacy encroachments. Two sources of public fears emanate from government surveillance or reprisals and private sector surveillance and unsolicited marketing practices. In the former case, fears for surveillance manifest through the extensive adoption of interception laws by most African governments, including anti-terrorism legislation with interception law provisions.

Surveillance and unsolicited communications for marketing from companies constitute another source of fear over privacy. Alongside these companies' surveillance, individuals also engage in minimum practices of surveillance and by sending unsolicited communications. In either case, the use of closed-circuit television (CCTV) at homes, offices, hotels and large shopping malls is now common in many places in Africa for the purpose of preventing crimes. These technologies are supplemented by SMS text messages. All of these have generated fears for loss of privacy.

HIV/AIDS: Privacy in the context of HIV/AIDS, perhaps, is the most notable area of rising privacy concerns in Africa. HIV/AIDS plagued the African continent in the 1980s. Since then, it has spread significantly. In 2019 there were 20,7 million people with HIV (54 per cent) in Eastern and Southern Africa, 4,9 million (13 per cent) in Western and Central Africa.[43] The epidemic had cost the lives of millions of people on the sub-continent. Efforts to prevent or provide care and support to people living with HIV have raised a number of privacy law issues. Consent to HIV testing is the most controversial issue surrounding privacy. Many people in Africa are concerned over HIV testing without their consent. Since there is no prevention of or cure for HIV, many people consider their health records in the context of HIV as most sensitive, fearing stigmatisation.[44] The second issue stemming from the first concerns the disclosure of HIV test results or status to third parties without authorisation of the persons concerned.

43 HIV Global Statistics, https://www.hiv.gov/hiv-basics/overview/data-and-trends/global-statistics (accessed 10 November 2021).

44 See, eg, SD Weiser and others 'Routine HIV testing in Botswana: A population-based study on attitudes, practices, and human rights concerns' (2006) 3 *PLoS Medicine* 1018-1019; NC Mbonu and others 'Stigma of people with HIV/AIDS in sub-Saharan Africa: A literature review' (2009) *Journal of Tropical Medicine* Article ID 145891, 14 pages doi:10.1155/2009/145891; P Anglewicz & J Chintsanya 'Disclosure of HIV status between spouses in rural Malawi' (2011) 23 *AIDS Care: Psychological and Sicio-Medical Aspects of AIDS/HIV* 100; The Wold Bank *Legal aspects of HIV/AIDS: A guide for policy and law reform* (2007), http://siteresources.worldbank.org/INTHIVAIDS/Resources/375798-1103037153392/LegalAspectsOfHIVAIDS.pdf (accessed 10 November 2021).

In response to the above concerns, some governments as well as private sector institutions in Africa such as Ghana, Kenya, South Africa and Tanzania have developed policies as well as special legislation. However, the major weakness of these laws and policies is that they focus on issues of confidentiality alone rather than privacy. Admittedly, while confidentiality is an aspect of privacy, confidentiality as such is inadequate to protect health records in the context of HIV. Apart from that, many of the laws are vague in terms of scope and ambit. Nevertheless, in relative terms concerns for privacy in the context of HIV in Africa has manifested through development of a larger corpus of case law on privacy.[45] Although such case law still falls short of the principles of data privacy, it serves to demonstrate how far Africans put significant weight on privacy of their health records.

Traumas of past injustices: The concepts of justice and injustice have been a subject of philosophical debates for centuries since the Plato's *Republic*.[46] Such debates are not covered here because of the little bearing they have on the issues addressed. Yet, it is sufficient to point out that an unjust system presupposes the existence of oppression, exploitation, repression, inhibition or restraints, whether at an individual or group level or by the state. In Africa, the most widely-cited traumas of past injustices are those relating to the system of apartheid in South Africa and the Rwandan genocide.[47] However, while these are commonly-cited examples of past injustices due to the magnitude of their effects, there are other past injustices in Africa. For example, the dictatorship of military rulers in Africa qualifies for the definition given above. Be that as it may, commentators are in agreement that privacy concerns are nourished by certain concrete experiences, such as the traumas of fascist oppression prior to and during World War II.[48] Banisar argues that one of the reasons

45 For a detailed review of case law on HIV/AIDS in African jurisdictions, see, eg, MT Ladan 'The role of law in the HIV/AIDS policy: Trend of case law in Nigeria and other jurisdictions' Inaugural lecture delivered at the Ahmadu Bello University, Zaria, Nigeria (2008) 19-22; MA Tadesse 'HIV testing from an African human rights system perspective: An analysis of the legal and policy framework of Botswana, Ethiopia and Uganda' LLM dissertation, University of Pretoria, 2007.

46 See, eg, D Sachs 'A fallacy in Plato's Republic' (1963) 72 *The Philosophical Review* 141-158; J Rawls 'Justice as fairness' (1958) 62 *The Philosophical Review* 164-194; WL McBride 'The concept of justice in Max, Engels, and others' (1975) 85 *Ethics* 204; JA Rawls *A theory of justice* (1971).

47 See, eg, G Weldon 'A comparative study of the construction of memory and identity in the curriculum of post-conflict societies: Rwanda and South Africa' (2003) 3 *International Journal of Historical Learning, Teaching and Research* 55; RU King 'Healing psychological trauma in the midst of truth commissions: The case of *Gacaca* in post-genocide Rwanda' (2011) 6 *University of Toronto Press Journals* 134-151.

48 Bygrave (n 5) 108.

for adopting privacy laws in many countries, including South Africa, is to remedy privacy violations that occurred under previous regimes and prevent those abuses from recurring.[49]

E-commerce: E-commerce in Africa is still evolving. Its current low level is a result of inadequate e-commerce infrastructure. Yet, where it has started to develop consumer trust and confidence, cyber-crimes and identity thefts have raised serious concerns. This is largely the result of e-commerce transactions collecting vast amounts of personal information. The 'Nigerian Advance Fee Scam' is the most popularly feared across Africa and even beyond, and has caused many privacy concerns in online commercial transactions.

World Summit on the Information Society-Tunis 2005: The World Summit on the Information Society (WSIS) involved a pair of United Nations (UN)-sponsored conferences about information, communication and, in broad terms, the information society that took place in 2003 in Geneva and in 2005 in Tunis. One of its chief aims was to bridge the so-called global digital divide separating rich countries from poor countries by spreading access to the internet in the developing world.[50] One of the principles of the WSIS in Geneva of 2003 states that '[t]he use of ICTs and content creation should respect human rights and fundamental freedom of others, including personal privacy, conscience, and religion in conformity with relevant international instruments'.[51]

Reaffirming the Geneva vision from an African perspective during the WSIS in Tunis (on 16 November 2005), the former President of South Africa, Mr Thabo Mbeki, made the following statement:

> Our country and continent are determined to do everything possible to achieve their renewal and development, defeating the twin scourges of poverty and underdevelopment. In this regard, we have fully recognised the critical importance of modern ICTs as a powerful ally we have to mobilise, as reflected both in our national initiatives and the priority programmes of NEPAD, the New Partnership for Africa's Development. We are therefore determined to do everything we can to implement the outcomes of this World

49 D Banisar 'Privacy and data protection around the world' Conference proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September 1999, 2, http://www.pcpd.org.hk/english/infocentre/conference.html(accessed 10 November 2021).

50 As above.

51 Geneva Declaration of Principles 2003, Principle 58, Document WSIS-03/GENEVA/DOC/4-E (12 December 2003), http://www.itu.int/wsis/docs/geneva/official/dop.html (accessed 10 November 2021)

> Summit on the Information Society and appeal to all stakeholders similarly to commit themselves to take action to translate the shared vision of an inclusive development-oriented information society in practical reality.[52]

The significance of the WSIS cannot be over-exaggerated. While it did not directly produce its effects over the people, it inspired African governments to commit themselves in using ICT in their development efforts. This also meant that African governments had or have to develop policies and regulations on ICT. To ensure that these commitments are made a reality, WSIS has established a monitoring procedure that periodically conducts follow-up on performance from a country to regional organisation level.[53]

International, regional and national data protection laws: International, regional as well as national policies and codes for protection of privacy have had impact on privacy in Africa. However, in relative terms, regional policies and codes have been more instrumental in influencing concerns over privacy in Africa and, consequently, the adoption of recent comprehensive data privacy legislation than others. In certain cases, international law offers inspiration for the development of particular domestic legislations or decision-making processes.[54]

At international level, three instruments may be identified that relate to the protection of the right to privacy: the Universal Declaration of Human Rights (Universal Declaration); the International Covenant on Civil and Political Rights (ICCPR); and the UN Guidelines, with regard to the protection of personal data. Since these instruments are UN instrument, they apply to African countries by virtue of their being members of the UN. However, their impact in shaping privacy ideas and consciousness as well as the adoption of policies and regulations has not been significant.

The only regional policy and code of privacy and data protection outside of Africa that has been influential in matters of privacy on the continent was the EU Directive 95/46/EC. It is imperative to mention that the Council of Europe Convention 108 with regard to automatic processing of personal data is the only European regional treaty open for accession by non-European states. Currently, Cape Verde, Mauritius, Morocco, Senegal and Tunisia are the only African states that have acceded to Convention

52 R Capurro 'Information ethics for and from Africa' (2007) 7 *International Review of Information Ethics* 2.

53 See, eg, ITU 'WSIS Forum 2011: Outcome Document' http://www.itu.int/wsis/implementation/2011/forum/inc/DocumentsWSISForum2011OutcomeDocument.pdf (accessed 10 November 2021).

54 As above.

108.[55] Burkina Faso has been invited to accede to the Convention 108 until 24 March 2022.[56] As has been the case elsewhere, Directive 95/46/EC exerted both political and economic pressure on African countries to adopt data privacy laws in the European style. Article 25 of Directive 95/46/EC provided that the transfer of personal data to third counties would only be allowed if such third countries maintained an adequate level of data protection law similar to the Directive. Yet, since the above European law entered into force in 1998, no African country has been declared as providing an 'adequate' level of protection of personal data. In 2010 some African countries that have implemented comprehensive data privacy laws applied to the EU for accreditation as satisfying this level of protection. Included in this list are Mauritius, Burkina Faso, Tunisia, Morocco and Senegal. While the reports for the rest of these countries have not been made public, that of Tunisia is publicly available. As already pointed out, the first report with regard to Tunisia data privacy law made it clear that Tunisia's regime is not adequate. The rest of the countries had similar outcomes although this was not directly stated in the reports.

In relation to the volume of personal data in the preceding paragraph, the prevailing view is that Africa needs to satisfy the requirements of the European Directive (and now the GDPR) in order to attract investment and outsourcing industries. The economic justification manifests in literature (journal articles, commentaries, reference books, newspapers, magazines and reports), legislation, bills, policies, Hansards, treaties and conventions as well as in *travaux préparatoires*. It is worth noting that the economic justification behind the adoption of data privacy legislation in Africa has also manifested in the reports for analysis of the adequacy of protection of personal data in some African countries.[57] Similarly, the justification was prominent in parliamentary discussions in Mauritian, Kenyan and in the South African legislative process.[58] As pointed out, there currently

55 Council of Europe 'Chart of signatures and ratifications of Treaty 108', https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=jESnZmay (accessed 10 November 2021).

56 Council of Europe 'Non-member states of the Council of Europe: Five years validity of an invitation to sign and ratify or to accede to the Council of Europe's treaties', https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22 (accessed 10 November 2021).

57 See, eg, CRID (Centre de Recherches Informatique et Droit), University of Namur (Belgium) 'Analysis of the adequacy of protection of personal data provided in Tunisia-Final Report' (2010) 7, http://alexandrie.droit.fundp.ac.be/GEIDEFile/6544.pdf?Archive=192619191089&File=6544_pdf (accessed 10 November 2021).

58 PMG., 'Protection of Personal Information Bill [B9-2009] briefing', 7th October 2009; http://www.pmg.org.za/report/20091007-protection-personal-information-bill-b9-2009-briefing (accessed 10 November 2021).; Portfolio Committee on Justice

is no general survey to concretise the extent to which African countries have economically been affected by the restriction on the transfer of personal data from Europe. In most cases, such claims have been made by sweeping statements. However, on country level, Morocco seems to have undertaken a study on the impacts of European data privacy law. In 2008 a report by the Moroccan Ministry of Economy pointed out that the low volume of relocation of banking and insurance services to Morocco was partly due to a lack of protection of personal data transferred to the kingdom, and recommended the adoption of legislation of this subject, which followed in 2009.[59]

3.2 Negative determinants

Lack of awareness of privacy risks: Privacy awareness reflects the extent to which an individual is informed about privacy practices and policies, about how disclosed information is used, and being cognisant about their impact over the individual's ability to preserve his private space.[60] A lack of privacy awareness perhaps is one of the most negative determinants that have impeded the growth of privacy concerns in Africa and, consequently, affecting the adoption of privacy policies and legislation. Understandably, this lack of individuals' awareness of privacy risks partly reflects the value Africans attach to privacy of their personal information. Sometimes privacy policies and legislation may exist in African countries, but ignorance by individuals produces the same result. Extending the concept of the 'privacy myopia' in the African context while explaining the value attached on privacy by individuals in Uganda, Bakibiknga argues that Ugandans largely suffer from 'privacy myopia'.[61] This also is the case in other African countries such as Nigeria, as explained by Kusamotu.[62] Yet,

and Constitutional Development., 'Background Information: Protection of Personal Information Bill [B9-2009], Deliberations 4th November 2009; http://www.pmg.org.za/report/20091104-protection-personal-information-bill-b9-2009-deliberations (accessed 10 November 2021).; Mauritius National Assembly, Debate No 12 of 01.06.04, Public Bills: Data Protection Bill (No. XV of 2004); Parliament of Kenya, The National Assembly, 'Hansard Report', Wednesday 6 November 2019.

59 Ministère de l'Economie et des Finances, Dé localisation des activités de services au Maroc, Etat des lieux et opportunités (Juillet 2008) 15, http://www.finances.gov.ma/depf/publications/en_catalogue/etudes/2008/delocalisation.pdf (accessed 10 November 2021).

60 H Xu and others 'Examining the formation of individual's privacy concerns: Toward an integrative view' International Conference on Information Systems (ICIS) Proceedings (2008) 6.

61 Bakibinga (n 15).

62 A Kusamotu 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European Union Directive 95/46' (2007) 16 *Information and Communications Technology Law* 157.

a lack of awareness of privacy risks should not be regarded as a natural phenomenon. There are a range of factors that offer an explanation for this situation. This includes a low level of computerisation or penetration of technology in Africa, resulting in the corresponding low level of data processing and awareness about its implications for privacy.[63] This penetration level has resulted into the 'digital divide' between urban and rural Africa.

A survey[64] by Ipsos has found that, compared to those living in developed nations, people in countries with lower economic living standards (Nigeria, Kenya and Tunisia) tend to have lower online privacy concerns with regard to personal information being monitored or bought and sold. Such individuals are also relatively less concerned about a general lack of privacy due to having so much information about themselves on the web. The survey further found that although over the past few years, developing nations have experienced some fast growth in the number of new internet users and smartphone owners, leading to exponentially sharper increases in the number of people who are newly exposed to online social networking, business transaction and e-commerce compared to nations with higher GDP per capita, privacy concerns have remained relatively low. The survey shows that increased familiarity with online experiences may not necessarily imply greater awareness of privacy issues or the ability to protect one's personal information. This is because most developing nations still have a nascent or poorly implemented institutional frameworks around data privacy. These findings are consistent with more recent surveys which have established that although Kenya, South Africa, Togo and Uganda have comprehensive data protection legislation, this is not necessarily a strong indicator of commitment to protection of privacy rights, or of efficacy of the legislative environment in ensuring the right to privacy and data protection.[65] Reports across these countries already indicate that an asymmetry between legislation and practice is evident at different levels. This is confirmed by a survey conducted by WorldWideWorx and commissioned by global technology company Zoho, which finds that 78% of South African businesses are unaware of privacy laws governing their marketing activities.[66]

63 As above.

64 EH Rho and others 'Differences in online privacy and security based on economic living standards: a global survey of 24 countries', Research Paper, Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK, 2018 at 11.

65 A Finlay 'Introduction and Overview' in *African Declaration on Internet Rights and Freedoms Coalition., Privacy and personal data protection in Africa: A rights-based survey of legislation in eight countries* https://africaninternetrights.org, May 2021, pp. 5-14.

66 Creamer Media Reporter (ed)., '78% of South African businesses are unaware about

Another factor affecting awareness is the high level of illiteracy in Africa.[67] With this general low illiteracy level, individuals' ability to understand threats posed upon their privacy becomes severely limited. However, this does not suggest that literate individuals are well placed to understand privacy risks to their personal information. A survey conducted across Africa, 'Awareness Survey on Freedom of Information and Data Protection Legislation and Open Government Data Initiatives'[68] from 27 to 30 September 2011 provides solid evidence that a lack of awareness of privacy risks affects a large number of literate individuals working in private sectors, governments, academic and researcher institutions.

Apart from the above factors affecting awareness, it is difficult to entirely disagree that African culture impacts on an individual's awareness and consciousness of privacy, particularly in rural areas where a collectivist life style is still discernible. As pointed out by some commentators, through group association in African cultures, an individual's interests are subordinate to those of groups. Accordingly, there is sharing of even sensitive personal information with others without being aware of the likely resulting privacy risks. Yet, while collectivist culture operates as a negative determinant, there has been rare discussion, let alone mention, of culture in the legislative processes and the *travaux préparatoires* to the data privacy laws leading to data protection legislation in Africa. This may partly be due to two main factors: over-dominance of economic justifications for adopting such legislation as state-sponsored agenda as well as its attendant propaganda and lack or inadequate public consultation during the legislative processes around data privacy laws.

Resistance to transparency: Some governments resist taking an interest in privacy issues as they do not wish to become more and more transparent and accountable to their citizens. The resistance may be demonstrated generally by the rejection of the bills of rights in the independent constitutions or restricting its application; the rejection of access of information legislation or the restriction of their application; and, specifically, being indifferent

privacy laws governing their marketing activities, rely heavily on third-party trackers and ad platforms – Survey' https://www.engineeringnews.co.za/article/78-of-south-african-businesses-are-unaware-about-privacy-laws-governing-their-marketing-activities-rely-heavily-on-third-party-trackers-and-ad-platforms-survey-2021-06-21

67 See, eg, UNESCO Institute for Statistics 'Adult and youth literacy' Fact Sheet (September 2011), http://www.uis.unesco.org/FactSheets/Documents/FS16-2011-Literacy-EN.pdf (accessed 10 November 2021).

68 K Taylor 'Awareness survey on freedom of information and data protection legislation and open government data initiatives' The Internet Governance Forum, Nairobi, Kenya, 27-30 September 2011 1-19, http://epsiplatform.eu/sites/default/files/IGF6_W123_PSISurveyreport_21October2011.pdf (accessed 10 November 2021).

in initiating the legislative process for data protection legislation, which in some ways places governments under certain obligations in processing personal information. This in turn limits the ability of governments to conduct unregulated surveillance over their people.

Lack of or inadequate legislative consultation: Historically, the drafting and enactment of data protection laws around the world, particularly in Europe, have frequently been lengthy processes fraught with controversy.[69] Yet, in some places, such as Sweden, the preparation and enactment of data protection legislation occurred relatively quickly and smoothly.[70] However, this does not suggest that data privacy legislation in Sweden was adopted without public consultation or in only few days. In Africa, with the exception of a few countries (such as South Africa and Kenya), the enactment of data privacy legislation had not engaged public consultation or such consultation had been inadequate. Ordinarily, public consultations in the legislative process generate debates about the necessity or otherwise of data privacy laws, their contents, enforcement, and so forth, which stimulates interest in and awareness about these laws to the public. Concomitantly, they facilitate the implementation of data privacy laws once enacted.

Cost: The costs of adopting and implementing comprehensive data protection legislation are also among critical issues for developing countries. Such costs are borne with respect to carrying out training, awareness-raising programmes, seminars, the conducting of investigations, dispute resolution, and so forth. As most African governments' annual budgets depend to over 30 per cent of budget support from donors,[71] it practically is difficult to finance the adoption and implementation of data privacy legislation.

4 Policy and regulatory frameworks for privacy and data protection

Policy and regulation of privacy and personal data protection in Africa can be considered at regional, sub-regional and national levels. At the regional level, various instruments have been developed under the auspices of the African Union (AU). Under sub-regional level there are initiatives by Economic Community of West African States (ECOWAS); the East

69 Bygrave (n 5) 4.

70 Bygrave (n 5) 5.

71 M Knoll 'Budget support: A reformed approach or old wine in new skins?' UNCTAD Discussion Papers 190 (October 2008) http://www.unctad.org/en/docs/osgdp20085_en.pdf (accessed 10 November 2021).

African Community (EAC); and the Southern African Development Community (SADC). Fewer initiatives are known to have taken place in the Common Market for Eastern and Southern Africa (COMESA) and Economic Community of Central African States (ECCAS), and Arab Maghreb Union (UMA).

4.1 The African Union

4.1.1 Human rights treaties

The African Charter on Human and Peoples' Rights (African Charter) is the main human rights treaty of the AU.[72] One of the objectives of the AU is to promote international cooperation having due regard to the Charter of the UN and the Universal Declaration.[73] This objective partly necessitated the adoption of the African Charter in 1981 in Africa. Concomitantly, the African Charter incorporates universal human rights standards and principles similar to those in the Universal Declaration. However, in contrast to the Universal Declaration, , the Africah Charter has its unique elements that reflect the virtues, culture and values of African traditions. First, the African Charter creates a reciprocal relationship between the individual and the community, linking individual and collective rights. Second, the African Charter creates a set of obligations that have to be fulfilled by an individual in order to enjoy the rights established.

As far as the protection of the right to privacy is concerned, the African Charter contains no express provision. This omission has erroneously led many commentators to conclude that Africans do not value privacy.[74] However, some commentators have advanced the argument that despite such an omission, privacy may still be read into other provisions, particularly the right to dignity.[75] Although this argument males sense, neither the African Commission on Human and Peoples' Rights (African Commission) nor the African Court on Human and Peoples' Rights (African Court), the main mechanisms under the African Charter, has so far provided an authoritative interpretation to that effect. This is despite the fact that the African Court has jurisdiction over all cases and disputes

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

73 OAU Charter 1963, art II(1).

74 See, eg, Gutwirth (n 11); Bygrave (n 12).

75 AB Enyew 'Regulatory legal regime on the protection of privacy and personal information in Ethiopia' LLM dissertation, University of Oslo, Norway, 2009 15, https://www.duo.uio.no/bitstream/handle/10852/22947/Binder1%5B1%5D.pdf?sequence=1&isAllowed=y (10 November 2021).

submitted to it concerning the interpretation and application of the African Charter, the African Court Protocol, and any other relevant human rights instrument ratified by the states concerned.[76]

There are limitations to the realisation of the rights stipulated under the African Charter generally through the available mechanisms. This is due to the fact that, although the African Commission has the power to receive complaints from individuals, its decisions are non-binding on a state party and, above all, they are considered confidential until they are approved for publication by the Assembly of Heads of State and Governments.[77] This is one of the reasons why the African Court was established. Interestingly, the African Court Protocol does not grant individuals direct access to the Court, as is the case with states and organisations. In this case, the African Court has a discretion to allow or disallow an individual to file a case.[78] Moreover, an individual cannot merely file a case to the Court if the relevant state has not made a declaration during the ratification of the Protocol, of accepting the jurisdiction of the Court to hear and determine such a case.[79]

The African Charter on the Rights and Welfare of the Child (African Children's Charter) is the only AU instrument that expressly guarantees the right to privacy. Article 10 of the Children's Charter states:

> No child shall be subject to arbitrary or unlawful interference with his privacy, family home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks.

The adoption of the African Children's Charter defeats the popular argument that the omission of a provision for protection of privacy in the African Charter is sufficient evidence to support the claim that Africans do not value privacy. However, one point must be clearly made, namely, that the main influence for the adoption of the African Children's Charter is the UN Convention on the Rights of the Child of 1989.[80] The right to privacy is one of the provisions in the UN Convention. Yet, it still is not

76 Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights, 2004 art.3 (African Court Protocol).

77 Art 59(1) African Charter.

78 Art 5(3) African Court Protocol.

79 Art 34(6) African Court Protocol.

80 United Nations Convention on the Rights of the Child 1989; adopted 20 November 1989 and entered into force 2 September 1990.

clear why the African Charter omits a clause on the protection of privacy despite the fact that it makes reference in its Preamble to the Universal Declaration and ICCPR that contain clear provisions on the protection of the right to privacy. The provisions on the rights to privacy in the Universal Declaration and ICCPR directly apply in some African countries of which the treaty practice is monism. Moreover, in dualist African states these provisions have also permeated into national constitutions after incorporation processes.

4.1.2 The African Union Convention

The AU Convention on Cyber Security and Personal Data Protection 2014 (Malabo Convention) is the continental binding treaty in the field of cybersecurity. The Convention was adopted by the twenty-third ordinary session of the Assembly, held in Malabo, Equatorial Guinea, on 27 June 2014. It just recently entered into force having obtained the fifteen ratifications required by its article 36.

The history of the Malabo Convention dates back to the Addis Ababa Declaration by the Heads of State and Government of the AU on 2 February 2010.[81] In this Declaration it was alluded to the fact that information and communication technologies (ICTs) are powerful catalysts for the development and integration process in Africa. However, it was realised that ICTs need to be regulated. Because of this, the establishment of a legal and regulatory framework that is harmonised and attractive to investments, shared telecommunications and ICT infrastructure as well as the convergence of networks, services and administration became necessary. In the context of the Addis Ababa Declaration, the Malabo Convention was adopted.

The Malabo Convention regulates three sets of issues: electronic transactions (chapter I); personal data protection (chapter II); and cybersecurity/cybercrimes (part III). Of interest in this part is the protection of personal data. One point has to be made clear from the outset. The Malabo Convention has been significantly influenced by the European data protection regimes, namely, the European Union Data

81 AU Addis Ababa Declaration on Information and Communication Technologies in Africa: Challenges and prospects for development, Assembly/AU/Decl.1(XIV), adopted by the 14th ordinary session of the Assembly in Addis Ababa, Ethiopia on 2 February 2010.

Protection Directive 95/46/EC, the Council of Europe Convention 108 and the OECD Guidelines.[82]

As far as the protection of personal data is concerned, the Malabo Convention requires each member of the AU to put in place a legal framework with a view to strengthening fundamental rights and public freedoms, particularly the protection of physical data, and punishing any violation of privacy without prejudice to the principle of the free flow of data.[83] Further, such mechanism must ensure that any processing of personal data respects the freedom and fundamental rights of natural persons while at the same time recognising the prerogatives of the state, the rights of local communities and the purposes for which businesses were established.[84]

The scope and application of the Malabo Convention are too broad.[85] It applies to data processing undertaken by private and public sectors. In both cases the Convention extends its application to processing of personal information of natural person and legal entities. Moreover, the Malabo Convention targets both automated and non-automated processing of personal data. The territorial application of the national data privacy is restricted to the processing of data taking place in the territory of a member state. Processing operations concerning public security, defence, state security and criminal law are also within the scope and application of the Convention. However, the Convention gives member states leverage to make exceptions under specific provisions of national legislation. Since the scope of these leverages is not clear, in practice a state may entirely exclude the application of the Convention on such types of data processing.

The Malabo Convention does not apply where processing takes place within the exclusive context of personal or domestic activity and where temporary copies are produced in the context of technical activities for transmission and access to a digital network for the sole purpose of offering other beneficiaries of the service the best possible access to the information so transmitted.[86] While the first exception in the Convention is similar to European data protection regimes, the former is further qualified, in that such data processing is not meant to be carried out for systematic

82 For a critical appraisal of the Malabo Convention, see generally LA Abdulrauf & CM Fombad 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67-97.

83 Art 8(1) Malabo Convention.

84 Art 8(2) Malabo Convention.

85 Art 9(1) Malabo Convention.

86 Art 9(2) Malabo Convention.

communication to third parties or for further dissemination. Practically, this additional qualification serves no value as any processing concealed to be undertaken under the cover of personal or domestic activities and subsequently discovered to be inconsistent with such purposes and limits will automatically be taken to fall short of this exception.

The Malabo Convention contains six data processing principles similar to EU data protection regimes.[87] The first principle is consent to and legitimacy of personal data processing. This principle does not apply in specific cases enumerated by the Convention. The second principle is the principle of lawfulness and fairness of personal data processing. The third is the principle of purpose, relevance and storage of processed personal data. Repurposing against the original purpose is restricted. The fourth principle is the principle of accuracy of personal data. The fifth principle is transparency of personal data processing. The sixth principle is confidentiality and security of personal data processing. The Convention also contains provisions on the protection of sensitive data.[88]

As it is conventional to most data protection regimes, the Malabo Convention contains rights of data subjects: the rights to information, access, object and rectification or erasure.[89] It also sets out obligations on data controllers. These include confidentiality, security, storage and sustainability obligations.[90]

Similarly, the Malabo Convention contains rules on transborder data movement. Article 14(6) of the Convention states that a data controller shall not transfer personal data to a non-member state of the AU unless such state ensures an adequate level of protection of privacy, freedoms and fundamental rights of persons whose data are being or likely to be processed. Surprisingly, the Convention neither provides criteria for assessing the level of adequacy of data protection, nor does it expressly indicate who is to undertake such assessment, although, this should be the national data protection authority. Institutionally, the Malabo Convention obliges every member of the AU to establish an authority with responsibility to protect personal data.[91]

87 Art 13 Malabo Convention.

88 Art 14 Malabo Convention.

89 Arts 16-19 Malabo Convention.

90 Arts 20-23 Malabo Convention.

91 Art 12(1) Malabo Convention.

4.2 Sub-regional frameworks

4.2.1 ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection

The Economic Community for West African States (ECOWAS) has 15 members.[92] ECOWAS was established by the Treaty of Lagos on 28 May 1975 with the objective of promoting cooperation and economic integration in the West African region through the harmonisation of policies and laws.[93]

In terms of data privacy protection, ECOWAS is the first and only sub-regional grouping in Africa to develop a concrete framework of data privacy law, namely, the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS. The Act has been strongly influenced by the EU Directive. In turn, the Supplementary Act has strongly influenced the Malabo Convention. The latter in fact has replicated the former word-to-word with only a few exceptions. Because of this, the analysis with regard to the Supplementary Act is unnecessary and the comments made above regarding the Malabo Convention apply.

It also is worth noting that contrary to the Malabo Convention, the Supplementary Act is an integral part of the ECOWAS Treaty.[94] Breaches of the Supplementary Act by member states can be enforced before the ECOWAS Court of Justice.

4.2.2 EAC Legal Framework for Cyber Laws 2008/2011

The East African Community (EAC) comprises six countries: Kenya, Uganda, Tanzania, Rwanda, Burundi and South Sudan. The Community was established in 1999 by the Treaty for Establishing of the East African Community 1999. The major aim of the EAC is to foster development among the member states. To this end, the EAC established a Customs Union in 2005 and a Common Market in 2010.

The EAC has not been isolated by the development of ICTs. The potential benefits and risks of using ICTs are issues that recently have gained prominent discussion in the EAC. In this regard, the realisation of a solid cyber law in the Community is essential in underpinning the

92 Benin, Burkina Faso, Cape Verde, Côte d'Ivoire, The Gambia, Ghana, Guinea, Guinea Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone and Togo.

93 Art 3 ECOWAS Treaty 1975.

94 Art 48 ECOWAS Supplementary Act 2010.

implementation of the Common Market Protocol, especially regarding services, an area of great potential for the region.[95] However, the sub-region as yet does not have a legal framework for the protection of personal data. Currently, only Kenya and Uganda have adopted comprehensive data protection legislation.

4.2.3 SADC Mode Law on Data Protection 2012

The Southern African Development Community (SADC) is a sub-regional grouping of 15 countries: Angola, Botswana, the Democratic Republic of the Congo (DRC), Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Seychelles, South Africa, Swaziland, Tanzania, Zambia and Zimbabwe. It was formed in Lusaka, Zambia, on 1 April 1980, following the adoption of the Lusaka Declaration. The main objectives of the SADC are to foster economic, political and social development in the member states.

As far as privacy and data protection is concerned, the SADC has adopted a model law on data protection in the sub-region, namely, the SADC Model Law on Data Protection 2012 (Model Law). The Model Law is heavily influenced by the European Directive 95/46/EC. However, there are significant differences in scope and ambit for the principles covered in these sets of laws. These are not considered here. It is important to note that the Model Law is not a binding instrument and, as such, it has little influence on law reforms in the sub-region.

4.3 National constitutions and data protection legislation

There are two main frameworks of protection of data privacy at national level in Africa: constitutions and statutory laws. The highest order of such protection is the national constitution of a respective country. In this category there are countries with express provisions for the protection of privacy in their constitutions.[96] This presents the largest group. The second group includes countries of which the constitutions lack express provisions on the constitutional right to privacy. For example, article 20 of the Angolan Constitution 2010 refers to the protection of personal integrity, the good name and reputation It is silent on privacy protection. The third group has constitutions that maintain two sets of provisions for

95 Dr Enos Bukuku, the EAC Deputy Secretary-General in charge of Planning and Infrastructure; see UNCTAD 'Press clipping: EAC develops cyber laws' (25 October 2011) http://r0.unctad.org/ecommerce/docs/EAC_Media.pdf (accessed 10 November 2021).

96 See, eg, Tanzania, Kenya, Nigeria, Mauritius, South Africa and Botswana.

the protection of privacy or personality right. The first set relates to the express provision of a constitutional right to privacy while, the second set is *habeas data*.[97]

As a basis for protecting privacy, a constitution has three limitations. First, the scope of the constitutional right to privacy depends on courts' interpretation on a case-to-case basis. This renders the law uncertain until the actual case has been filed in court. Currently this case law is scant (South Africa, Kenya, Uganda, Tanzania, Mauritius) or lacking in some jurisdictions. Second, in most cases constitutions only protect against infringements of privacy committed by the state and its agencies. The private sector is excluded. Since the private sector is fast growing and expanding in Africa, constitutional protection does not prevent the misuse of personal information by businesses and private sector entities. Third, infringements of the constitutional right to privacy attract different remedies from those obtained under data protection legislation. For example, monetary compensation is not a remedy under breaches of constitutional provisions.

Apart from constitutional protection, there are also statutory protections. These are either by comprehensive data protection legislation, sectoral laws or *ad hoc* provisions in different statutes. Currently there are 30 African countries with comprehensive data protection legislation.[98] With the exception of the recently-adopted data protection legislation, which is based on the European General Data Protection Regulation, the rest of the data protection laws are based on the now-repealed European Union Data Protection Directive 95/46/EC. The main manifestations of sectoral law protecting privacy are those in the communications sector, health and employment. However, in most cases these sectoral laws fail to address specific principles in the relevant sector. This is the case, for example, in the employment sector and the requirements of the mandatory or concealed pre-employment HIV test by employers. In case of *ad hoc* provisions, the laws contain only few sections that may have a privacy implication.

There finally is protection of privacy through the common law. This form of privacy protection is clearly available in a few African countries (for instance, South Africa). South Africa currently is the only African

97 See, eg, Cape Verde and Angola.

98 Algeria, Angola, Benin, Botswana, Burkina Faso, Cape Verde, Chad, Congo-Brazzaville, Egypt, Equatorial Guinea, Gabon, Ghana, Guinea Conakry, Côte d'Ivoire, Kenya, Lesotho, Madagascar, Mali, Mauritania, Mauritius, Morocco, Niger, Nigeria, São Tomé and Príncipe, Senegal, Seychelles, South Africa, Togo, Tunisia, Uganda.

jurisdiction that has a relatively large corpus of case law on common law privacy. However, such case law does not offer prescriptive guidance in terms of the scope and ambit of principles.

5 Analysis of data privacy policies in Africa: Patterns and trends

As pointed out, 30 out of 55 African countries have adopted data protection legislation. Cape Verde is the first African country to enact data protection legislation in 2001. The latest country to adopt data protection legislation is Egypt (July 2020). The following is the analysis of the major trends/ patterns of the African data privacy legislation and practice:

- *Inspired by EU-data protection governance*

Data privacy laws in Africa (national, regional and continental) are largely inspired by the EU data protection regime, mainly the now-repealed Data Protection Directive 95/46/EC. Articles 25-26 of this Directive comprised the restriction of data export outside EU to third countries without an 'adequate level' of protection. Since the rest of the world, including Africa, has trade relations with EU countries, the 'adequacy requirement exerted indirect pressure on African countries to enact data protection legislation based on the EU style.

With the repeal of the Data Protection Directive and its replacement by the GDPR, some African countries have revised their laws to match up with the GDPR standards (for instance, Mauritius). However, countries that adopted data protection after the GDPR has been in force have attempted to enact such laws in compliance with the GDPR (for instance, Uganda, Kenya, Egypt). It is worth noting that, although South Africa adopted its data protection legislation (POPIA) in 2013, almost five years before the GDPR entered into force, it took into consideration provisions of the early texts of the GDPR. Hence, it is mostly based on the GDPR.

It is noticeable that EU through its institutions, CoE, the United Nations Conference on Trade and Development (UNCTAD), and ITU through various programmes offered technical support to Africa to assist African governments to put in place data protection legal frameworks. This means that there still is limited capacity in Africa to adopt data privacy laws. Yet, this questions how issues of context are handled in law reform processes.

- *Little influence of African constitutions, continental and regional privacy policies*

Most objective clauses of data protection bills/laws in African countries stipulate that one of the reasons for adopting data privacy legislation is 'to give effect to a constitutional provision on the right to privacy'. However, the value of the constitutional right to privacy is questionable. It certainly is known that at independence in the 1960s and 1970s, many African countries adopted constitutions with a bill of rights that included an express provision on the right to privacy. However, for more than 40 years such provisions on the right to privacy have never been implemented by legislation, nor have such provisions been litigated upon to result in strong privacy jurisprudence except on a very limited scale (for instance, in South Africa, Kenya, Nigeria, Uganda and Tanzania).

Likewise, Africa has put in place binding data privacy treaties/agreements such as the African Union Convention on Cyber Security and Personal Data Protection 2014 and the ECOWAS Supplementary Act on Personal Data Protection 2010. There are also non-binding instruments (soft law) such as SADC Model Law on Data Protection 2012; the EAC Framework for Cyberlaw I, 2010; the ECCAS Model Law on Data Protection 2013; and the AU/Internet Society Personal Data Protection Guidelines for Africa 2018.

Overall, the above instruments have similar provisions with slight wording. They have also been influenced by the European data protection regimes. As pointed out, AU and ECOWAS instruments are the only binding agreements, while the rest constitute soft law. The issue is to what extent African regional and continental instruments have been influential to the data privacy law reform in Africa. It is difficult to see any such influence. The AU Convention was adopted in 2014. So far it has not entered into force for want of 15 ratifications. Five years have now lapsed since the Convention was adopted without it entering into force. Which influence then could it provide? Inspirational or what? Assuming that the Convention had already been in force, it lacks equivalent institutions such as those in the GDPR/EC Directive 95/46/EC which could monitor compliance. This also is the limitation with respect to the ECOWAS Supplementary Act on Personal Data Protection. Moreover, the preparatory documents of data privacy law in African countries indicate no reference to the African continental and regional privacy policies. Instead, express reference and detailed discussion is made to the European privacy regime by then EC Directive 95/46/EC (repealed) and now the GDPR. Moreover, in 2010 four African countries (Burkina Faso, Mauritius, Tunisia and Morocco) attempted to seek accreditation of

their data protection systems to the EU.[99] As pointed out, a preliminary assessment indicated that they all fell below the EU adequacy standards. Renewed efforts by these states and others in Africa to race to Europe are now being made through accession to the CoE Convention 108 as an alternative route, which appears to be less stringent to comply.[100]

- *Flawed law reform process*

It is interesting to note that with the exception of a few countries, data protection and law reform in Africa has largely been an exercise of copy and paste of European law.[101] This is attributed to a number of reasons: a lack of competent experts in the area of data privacy law; a lack of interest and avoidance of cost by governments to invest in the reform process; attempts to show to Europe that national legislation are strictly according to the Directive 95/46/EC or GDPR, hence facilitating accreditation of such legislation, and so forth. Concomitantly, in many African countries privacy law reform is simply about legal drafting and nothing more. There normally is a lack of and/or limited debates and public consultation. The second EU consultant notes that 'much of the existing legislation(in Mauritius) was copied from much larger countries, notably United Kingdom, New Zealand and South Africa, without a thorough analysis of the actual needs and capacities of Mauritius, and without much learning from the experiences of other small island developing states'.[102] While borrowing and legal transplantation are acceptable and perhaps are inevitable in the field of data privacy law, the domestication of European law into the African context is not only important but necessary. Greenleaf correctly observes that 'most striking, the African regional framework (as well as national legislation) does not display any African-specific approach to data protection'.[103] However, attempts to domesticate such laws must be done with caution. The Nigerian and Kenyan (first drafts) data privacy

99 AB Makulilo 'Data protection regimes in Africa: Too far from European "adequacy" standard?' (2013) 3 *International Data Privacy Law* 42-50.

100 AB Makulilo 'African accession to Council of Europe Privacy Convention 108: Moving towards stronger privacy protection' (2017) 41 *Datenschutz und Datensicherheit-DuD* 364-367.

101 AB Makulilo 'Data protection and law reform in Africa: A systematic or flawed process?' (2016) 2 *International Journal of Technology Policy and Law* 228-241.

102 Confidential report 'Ensuring the compliance of the data protection legislation and principles of Mauritius with EU standards, 2011' 4.

103 G Greenleaf & B Cottier 'Comparing African data privacy laws: International, African and regional commitments' University of New South Wales Law Research Series (2020) 33, https://ssrn.com/abstract=3582478 or http://dx.doi.org/10.2139/ssrn.3582478 (accessed 10 November 2021).

Bills demonstrate poor examples as they contain limited provisions with regard to processing personal data.[104]

- *Lack of international harmonisation*

As data-processing operations increasingly extend across national boundaries, the way in which they are to be regulated should take account of the way in which they are regulated in a wide variety of countries, such consideration being one precondition for achieving harmonised regulation.[105] With respect to Africa, Makulilo has extensively discussed the challenges of harmonisation of data privacy policies.[106] Chiefly among these is the existence of multiplicities of regional privacy policies. Even though such policies contain similar provisions, it is difficult for them to drive Africa towards a common point. As pointed out, most of the instruments are non-binding while only the ECOWAS Supplementary Act and AU Convention are binding. Similarly, it has been pointed out that the AU Convention has not yet entered into force. The other reason is the lack of centralised institutions to monitor compliance with the policies, especially the AU Convention. There also is the question of existing different legal systems among the participating countries in regional economic communities (RECs) and at the AU level, which has led to somewhat divergent legislative practices and procedures between the groups of countries. These legal systems are largely made up of the common and civil law legal systems.

- *Lack of and/or weak enforcement*

This is one of the aspects that raises many questions about the value of data privacy in Africa. So far 12 out of 30 African countries with data privacy legislation have not yet appointed data protection authorities.[107] While there is no particular standard time for a data protection authority to be appointed, six out of the 12 African countries have so far continued

104 AB Makulilo 'Nigeria's Data Protection Bill: Too many surprises' Privacy Laws and Business International Report, 2012, No 120 25-27; Article 19 'Nigeria: Personal Information and Data Protection Bill', http://www.article19.org/resources.php/resource/3683/en/nigeria:-personal-information-and-data-protection-bill (accessed 10 November 2021). Article 19 'Kenya: Draft Data Protection Bill critically limited', http://www.article19.org/resources.php/resource/2825/en/kenya:-draft-data-protection-bill-critically-limited (accessed 10 November 2021).

105 Bygrave (n 5) 12.

106 AB Makulilo 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer, Law and Security Review* 78-89.

107 Algeria, Botswana, Chad, Congo Brazzaville, Egypt, Equatorial Guinea, Guinea Conakry, Madagascar, Mauritania, Niger, Seychelles, Togo.

for one to four years without a data protection authority in place.[108] One may argue that this is still a reasonable time. However, the other six African countries have taken a minimum of five to a maximum of 16 years without appointing a data protection authority.[109] Cape Verde, the first African country to adopt data protection legislation in 2001, only appointed a data protection authority in 2017, after 16 years. Seychelles, the second African country to adopt data protection legislation, has to date not brought its law into force. South Africa, which passed its data protection legislation in 2013, has only brought the substantive part of the law in force in 2020, almost seven years later.

It is also important to note that the majority of countries with appointed data protection authorities have not done much as far as enforcement is concerned. In 2012, 2014 and 2020 Makulilo closely analysed the enforcement of the data protection legislation in Mauritius based on the repealed law (2004) and the new legislation (2017). He came to the conclusion that although Mauritius is doing well regarding enforcement, a number of shortcomings have to be addressed. One of the issues about which the data protection authority is complaining is inadequate resources (both financial and human) to support the activities and functions of the authority. In the beginning, the interpretation of the law based on complaints referred to the data protection authority was not consistent in similar complaints and at times other considerations outside the data protection legislation were taken into account. However, under the new data protection legislation there is consistency in the interpretation of similar complaints.

6 Conclusion

This chapter has illustrated that after a lapse of two decades, significant developments have taken place in Africa as far as data protection is concerned. First and foremost, there has been a steady increase and interest of many African governments to adopt data privacy policies and laws. Second, there have been attempts to harmonise data privacy laws and policies across Africa through the adoption of a continental treaty on data privacy as well as sub-regional levels. Also, important to note, African governments have gained interest to accredit their data protection systems to the most advanced, particularly those in Europe, in order to facilitate free flow of personal information. This in turn may boost African economies through foreign investment. However, the growth and development of data privacy in Africa still faces critical challenges, as discussed above.

108 Algeria, Botswana, Congo Brazzaville, Egypt, Niger, Togo.

109 Cape Verde, Chad, Guinea Conakry, Madagascar, Mauritania, Seychelles.

Nonetheless, there are still prospects for African governments to address such challenges through international cooperation.

References

Abdulrauf, LA & Fombad, CM 'The African Union's Data Protection Convention 2014: A possible cause for celebration of human rights in Africa?' (2016) 8 *Journal of Media Law* 67

Anan, K 'What is my beef against SIM card registration in Ghana? Independent Civil Advocacy Network (25 January 2010), http://www.i-can-ghana.com/?p=104 (accessed 10 November 2021)

Anglewicz, P & Chintsanya, J 'Disclosure of HIV status between spouses in rural Malawi' (2011) 23 *AIDS Care: Psychological and Socio-Medical Aspects of AIDS/HIV* 998

Bakibinga, EM 'Managing electronic privacy in the telecommunications sub-sector: The Ugandan perspective' (2004) http//:thepublicvoic.org/eventscapetown04/bakibinga.doc (accessed 10 November 2021)

Banisar, D 'Linking ICTs, the right to privacy, freedom of expression and access to information' (2010) 16 *East African Journal of Peace and Human Rights* 124

Banisar, D 'Privacy and data protection around the world' Conference Proceedings of the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, 13 September 1999 1, http://www.pcpd.org.hk/english/infocentre/conference.html (accessed 10 November 2021)

Bennett, CJ *Regulating privacy: Data protection and public policy in Europe and the United States* (Cornell University Press 1992)

Bygrave, LA *Data protection law: Approaching its rationale, logic and limits* (Kluwer Law International (2002)

Bygrave, LA 'Privacy protection in a global context: A comparative overview' (2004) 47 *Scandinavian Studies in Law* 319

Bygrave, LA *Data privacy law: An international perspective* (Oxford 2014)

Capurro, R 'Information ethics for and from Africa' (2007) 7 *International Review of Information Ethics* 1

Enyew, AB 'Regulatory legal regime on the protection of privacy and personal information in Ethiopia' LLM dissertation, University of Oslo, Norway, 2009

EPIC Alert 'EPIC Hosts Privacy and Public Voice Conference in Africa' (23 December 2005) Vol 11, No 24, http://www.epic.org/alert/EPIC_Alert_11.24.html (accessed 10 November 2021)

Evrensel, A 'Introduction' in Evrensel, A (ed) *Voter registration in Africa: A comparative analysis* (EISA 2010) 1

Greenleaf, G & Cottier, B 'Comparing African data privacy laws: International, African and regional commitments' University of New South Wales Law Research Series (2020), https://ssrn.com/abstract=3582478 or http://dx.doi.org/10.2139/ssrn.3582478. (accessed 10 November 2021)

Gross, H 'The concept of privacy' (1967) 42 *New York University Law Review* 34

Gutwirth, S *Privacy and the information age* (Lanham/Boulder/New York/Oxford/Rowman & Littlefield Publ 2002)

Izuogu, CE 'Data protection and other implications in the ongoing SIM card registration process' (2010), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597665 (accessed 10 November 2021)

King, RU 'Healing psychological trauma in the midst of truth commissions: The case of Gacaca in post-genocide Rwanda' (2011) 6 *University of Toronto Press Journals* 134

Knoll, M 'Budget support: A reformed approach or old wine in new skins?' UNCTAD Discussion Papers 190 (October 2008) 1

Kusamotu, A 'Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European Union Directive 95/46' (2007) 16 *Information and Communications Technology Law* 149

Ladan, MT 'The Role of Law in the HIV/AIDS Policy:-Trend of Case Law in Nigeria and Other Jurisdictions', Inaugural Lecture delivered at the Ahmadu Bello University, Zaria, Nigeria, 2008, pp 1-64

Makulilo, A.B., 'African accession to Council of Europe Privacy Convention 108: Moving towards stronger privacy protection' (2017) 41 *Datenschutz und Datensicherheit-DuD* 364

Makulilo, AB 'Data protection and law reform in Africa: A systematic or flawed process?' (2016) 2 *International Journal of Technology Policy and Law* 228

Makulilo, AB 'Data protection regimes in Africa: Too far from European "adequacy" standard?' (2013) 3 *International Data Privacy Law* 42

Makulilo, AB 'Myth and reality of harmonisation of data privacy policies in Africa' (2015) 31 *Computer, Law & Security Review* 78

Makulilo, AB 'Nigeria's Data Protection Bill: Too many surprises' (2012) *Privacy Laws & Business International Report* 25

Makulilo, AB 'Registration of SIM cards in Tanzania: A critical evaluation of the Electronic and Postal Communications Act, 2010' (2011) 17 *Computer and Telecommunications Law Review* 48

Makulilo, AB 'The quest for information privacy in Africa' (2018) 8 *Journal of Information Policy* 317

Mbonu, NC and others 'Stigma of people with HIV/AIDS in sub-Saharan Africa: A literature review' *Journal of Tropical Medicine* 2009, Article ID 145891, 14 pagesdoi:10.1155/2009/145891

McBride, WL 'The concept of justice in Max, Engels, and Others' (1975) 85 *Ethics* 204

Neethling, J and others *Neethling's law of personality* (LexisNexis 2005)

Neethling, J and others *Neethling's law of personality* (Butterworth 1996)

Neethling, J 'Die reg op privaatheid' LLD thesis, UNISA, 1976

Neethling, J 'The concept of privacy in South African law' (2005) 122 *South African Law Journal* 18

Rawls, J 'Justice as fairness' (1958) 62 *The Philosophical Review* 164

Rawls, J *A theory of justice* (Harvard University Press 1971)

Roos, A 'Data protection: Explaining the international backdrop and evaluating the current South African position' (2007) 124 *South African Law Journal* 400

Roos, A 'The law of data (privacy) protection: A comparative and theoretical study' LLD thesis, UNISA, 2003

Sachs, D 'A fallacy in Plato's Republic' (1963) 72 *The Philosophical Review* 141

Sutherland, E 'The mandatory registration of SIM cards' (2010) 16 *Computer and Telecommunications Law Review* 61

Tadesse, MA 'HIV Testing from an African human rights system perspective: An analysis of the legal and policy framework of Botswana, Ethiopia and Uganda' LLM dissertation, University of Pretoria, 2007

Warren, SD & Brandeis, LS 'The right to privacy' (1890) 4 *Harvard Law Review* 193

Weiser, SD and others 'Routine HIV testing in Botswana: A population-based study on attitudes, practices, and human rights concerns' (2006) 3 *PLoS Medicine* 1013

Weldon, G 'A comparative study of the construction of memory and identity in the curriculum of post-conflict societies: Rwanda and South Africa' (2003) 3 *International Journal of Historical Learning, Teaching and Research* 55

Xu, H and others 'Examining the formation of individual's privacy concerns: Toward an integrative view' International Conference on Information Systems (ICIS) Proceedings (2008) 1