Giving "teeth" to the African Union towards advancing compliance with data privacy norms

Lukman Adebisi Abdulrauf ORCID: https://orcid.org/0000-0003-4877-9415*

Department of Public Law, University of Ilorin, Nigeria and Institute for International and Comparative Law in Africa (ICLA), Faculty of Law, University of Pretoria, South Africa

Abstract

That international organisations have always played a pivotal role in the development and advancement of data privacy norms is now beyond doubt. This is why the law of international institutions is critical for data privacy law. The Council of Europe (CoE), the Organisation for Economic Cooperation and Development (OECD), and the European Union (EU) for example have been global pacesetters in advancing data privacy norms not only in terms of having notable instruments but also ensuring compliance with data privacy norms by state parties. Concerning advancing compliance specifically, the role of these international organisations cannot be overemphasized. Although data privacy is no longer new to Africa, compliance with data privacy norms has been significantly lower compared to other jurisdictions. A (possible) explanation for this is that the primary regional organisation on the continent – the AU – has played an insignificant role in this regard. There seems to be no basis for this view considering that the AU has also made an international treaty on data privacy. This singular fact, forecloses any contention that the absence of a settled source of data privacy norms in Africa is a reason for the low level of compliance. Nevertheless, while there is now a data privacy standard by the AU, several questions arise. First, why has compliance with data privacy norms on the continent been so weak? Second, how can the AU advance the proper compliance with data privacy norms like its counterpart, the EU, despite its different architecture? Using insights from the normative and institutional theories of state compliance, the article suggests how to strengthen the AU toward advancing compliance with data privacy norms.

Keywords: data privacy norms; international data privacy law; normative framework; Compliance; African Union; African states

1. Introduction

This article focuses on reinforcing the African Union (AU) towards advancing compliance with data privacy norms among member states. It specifically interrogates the issue regarding why the AU is not so influential in issues of data privacy given how active international institutions have been in the field. The contribution, therefore, attempts an explanation of the current state of affairs despite the recently adopted Data Protection Convention[1] by the regional

* E-mail: lukmanrauf@gmail.com abdulrauf.la@unilorin.edu.ng

[1] The African Union Convention on Cyber Security and Personal Data Protection 2014 available at https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf accessed 31 October 2020.

organisation. Recently, issues on data privacy have provoked significant global debate. No thanks to Snowden's revelations in 2015, the world has come to be aware of the nature and extent of mass surveillance and data mining by state governments (and private entities). This has made data privacy a hot issue for global debate leading to significant attention to the field. Besides, the rapid advances in technology which has facilitated easy access to individuals' personal information have also made data privacy increasingly under scrutiny. This phenomenon is said to be one of the greatest challenges of our time especially with the ubiquitous nature of information society. The information society and the technological advances witnessed in most countries have exposed the need for legal and policy initiatives to protect individuals' personal information using human rights instruments. Indeed, this is because an individual's personal data is taken as a representation of his/her person and should therefore be accorded the necessary human rights protection using an appropriate legal framework. Over time, efforts to protect individuals with regard to the processing of their personal information have been championed by international institutions with international legal sources. This is no surprise considering the way and manner information technology contributes to undermining borders and the trans-border nature of personal information processing.[2] This is also a reason why international organisations play a more active role in this field. While international organisations like the EU and the CoE have been very proactive in this regard, the same cannot be said of the AU.[3] Apart from adopting the AU Convention on Cyber Security and Personal Data Protection (hereinafter AU Data Protection Convention or Data Protection Convention), nothing else has been done by the international institution to signify its seriousness in this increasingly sensitive and crucial field of law. Having a normative framework is one thing and eliciting compliance is another. Without specific measures to induce compliance, a framework remains like a 'dead letter' law.

The AU's silence in this field is particularly perplexing given that Africa too is home to some of the most pervasive surveillance programs and data mining activities. For example, in a recent report, it was established that African governments are increasingly requesting users' personal information from social network companies such as Google, Facebook and Twitter obviously in violation of data privacy norms.[4] With the nature and extent of mass-surveillance and data mining that takes place across the world and even in Africa, it is time to reassess the role (or potential) role of the AU in promoting compliance with data privacy norms. Remarkably, the crux of the issue here is not so much about the instrument in place but the quality of implementation and enforcement of the law. Domestic measures have only been relatively successful when supplemented with international initiatives. It is in this respect that one can appreciate the role of the EU as 'guardians of data privacy right' in Europe.[5] A common belief is that international institutions cannot do much in the enforcement of

[2] P de Hert and V Papakonstantinou, 'Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably a UN Agency?' (2013) 9(2) *I/S: A Journal of Law and Policy* 274.

[3] For a general trajectory of the works and influence of other international organisations in the field of data privacy law, see de Hert & Papakonstantinou (n 2) 285-288. African initiatives are however surprisingly missing in this discussion.

[4] Y Kazeem, 'African governments are requesting more data from Facebook, Google, and Twitter than ever before' https://qz.com/africa/1064168/african-governments-user-data-requests-from-facebook-google-and-twitter-hits-historic-level/ accessed 31 October 2020.

[5] See H Hijmans, *The European Union as guardian of internet privacy* (Springer, Switzerland 2016).

international norms since enforcement is for domestic institutions.[6] While this may be true, it is argued in this article that there is much more international institutions can do especially since states/government are the worst violators.

It is apposite to acknowledge the challenge that may exist in looking unto EU mechanisms of compliance to draw lessons for the AU. This is because although the AU is 'modeled almost entirely' after the EU, they do not have a similar architecture in terms of norms implementation and enforcement. The AU is an intergovernmental organisation rather than a supranational organisation like the EU.[7] The practical implication of this is that it does not wield so much power over state parties to compel compliance with their international/regional obligations as the EU does. Be that as it may, we contend that the AU, being the foremost regional body in Africa, can still take some lessons especially in the field of privacy. This is because of how influential the EU has been in this regard.

The article proceeds as follows. After the introduction in Part I, Part 2 critiques the normative framework on the right to data privacy in Africa and the applicable legal regime. Part II considers the possible challenges the AU may face in the process of obtaining states' compliance with data privacy norms. While using the main theories of compliance with data privacy norms, especially the normative and the institutional theories, the challenges are analysed from two perspectives: challenges with the normative framework and challenges brought about by the structure of the AU. The foregoing discussion presents a formidable platform to analysing the available means to strengthen the AU towards being more effective in obtaining states' compliance with the African data privacy standards. The last part concludes the article with a brief reflection on why the AU must seriously begin to play a more active role in ensuring the realisation of the right to data privacy.

2. A critique of the normative framework on data privacy in Africa

Before considering the normative framework on data privacy in Africa, it is important to explain what data privacy norms are and the more vexed issue of whether they have indeed crystallized into a norm of public international law.

2.1. What are data privacy norms?

Data privacy norms[8] are a set of rules which are established to protect individuals from the effects of the illegal or arbitrary processing of their personal information. In today's world of

[6] According to Koh, 'international rule are rarely enforced, but usually obeyed.' HH Koh, 'Why do nations obey international law? (June 1997) 106(8) The Yale Law Journal 2603.

[7] For an in-depth discussion of the EU and its supranational character, see RJ Goebel, 'Supranational? Federal? Intergovernmental? The Governmental structure of the European Union after the Treaty of Lisbon', (2013) 20(1) Columbia Journal of European Law 78-141.

[8] Reference to data privacy as a norm is uncommon in the literature on the subject matter. While the term 'norms' has various meanings, it is used here to refer to 'a widespread or usual practice, procedure, or custom'. See Merriam-Webster Dictionary https://www.merriam-webster.com/dictionary/norm accessed 31 October 2020. For examples of literature that use data privacy as a norm, see MD Birnhark, 'Soft legal globalization: the role of the EU Data Protection Directive in the emerging global data protection regime' (2008) https://www.tau.ac.il/law/minerva2/Birnhack.pdf accessed 31 October 2020; M Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance* (Hart Publishing, Oxford 2017).

'big data' and increasing loss of control over one's personal data, individuals are exposed to certain harm as a result of the use of their personal information (processing) for purposes which they never envisaged. It is in this respect that data protection law creates a rule for individuals to retain control to ensure that their personal information is only used in a rights-respecting manner. The control paradigm is what has made contemporary scholarship argue that data protection is different from the right to privacy especially.[9] While this position has been so contentious over time in other parts of the world, the position is clearer in the EU especially with an explicit right of data protection different from the right to privacy in the Treaty for the Functioning of the European Union (TFEU) and most importantly, the EU Charter.[10] Brkan argues that in the EU, '[t]he right is not only expanding…but also gradually gaining importance compared to other fundamental rights and competing interests.'[11] As if to put the debates to rest, the UN's increasing interest in the field, especially with two recent General Assembly's (GA) resolution on *the right to privacy in the digital age* and the creation of the mandate for a UN Special Rapporteur on the right to privacy,[12] has made it clear that the UN also recognises the need to protect individuals in the context of the use of their personal information.[13] Specifically, these resolutions call upon states

> [t]o review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;[14]

Although this protection is to be carried out within the right to privacy paradigm under the UDHR and ICCPR, the UN in a way recognizes the *sui generis* nature of such protection that may require unique rules and even the establishment (and maintenance) of independent oversight mechanism.[15] As a resolution of the UN GA, it indeed carries significant weight under international law.[16]

Data privacy, as it is usually said, comprises of certain key rules on the handling of information which falls under the category of 'personal information/data.' The essence of the rules is to

---

[9] See for example, O Lynskey, 'Deconstructing data protection: The "added-value" of a Right to Data Protection in the EU Legal Order (2014) 63(3) ICLQ 569-579.

[10] See for example M Tzanou, 'Data Protection as a Fundamental Right Next to Privacy? 'Reconstructing' a not so New Right' (2013) 3(2) International Data Privacy Law 88-99.

[11] M Brkan, 'The unstoppable expansion of the EU Fundamental right to data protection: little shop of horrors?' (2016) 23(5) Maastricht Journal of European and Comparative Law 812.

[12] See G Greenleaf, 'The UN Special Rapporteur: Advancing a global privacy treaty' (2015) 136 Privacy & Business International Report 7-9.

[13] See UNGA Resolution A/RES/68/167 on '*The right to privacy in the digital age'* http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 and UNGA Resolution A/RES/69/166 accessed 31 October 2020 on '*The right to privacy in the digital age'* https://undocs.org/en/A/RES/69/166 accessed 31 October 2020. For more critical assessment on the UN initiatives toward protection of data privacy rights in the digital age, see C Nyst & T Falchetta, 'The right to privacy in the digital age' (2017) 9(1) Journal of Human Rights Practice 104.

[14] See para 4(c) of the Resolution.

[15] See para 4(d) of the Resolution.

[16] See MD Öberg, 'The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ' (2005) 16(5) European Journal of International Law 879.

protect individuals (usually called 'data subjects') from harm resulting from the manual or automated processing of their personal information by the state of private entities (usually called 'data controllers'). 'Processing' in this respect refers to all sort of activities which can be performed on/with individuals' personal information such as its collection, storage, transmission, etc. Succinctly, the rules include a set of basic principles on information handling generally known as 'Fair Information Principles' and a set of data privacy rights for individuals.[17] Among the norms is also the requirement for the establishment of a specialized agency for the enforcement of the principles usually termed Data Protection Authorities.

Some more comments about the basic principles are in order. First, these principles have been aptly described as 'the pith and basic thrust' of data privacy law and are contained in almost all data privacy instruments with little or no variations.[18] Second, there is no particular order of these principles in the data privacy instruments. It all depends on the style adopted by the draftsman. The implication of this is that no principle is superior to another as they each have a normative force of their own. Third, these basic principles as succinctly captured by Lee Bygrave are Fair and lawful processing;[19] proportionality;[20] minimality;[21] purpose limitation;[22] data subject influence;[23] data quality;[24] data security;[25] and sensitivity.[26] Although these principles may be of equal status, the EU Charter of Fundamental Rights (EU Charter) seems to place more emphasis on some of them. After providing for the general right to data protection in Article 8(1), subsections (2) & (3) stipulated that:

> Such data must be processed *fairly for specified purposes* and on the basis of the *consent of the person concerned* or some other legitimate basis laid down by law. Everyone has

[17] de Terwangne made an analysis of some of these key principles which he termed 'universal'. It is submitted that the principles identified by the author are not that different from what Bygrave discussed above. See C de Terwangne, 'Is a Global Data Protection Regulatory', in S Gutwirth *et al* (eds), *Reinventing data protection* (Springer, Dordrecht 2009) 175.
Model Possible?

[18] L Bygrave, *Data privacy law: An international perspective* (OUP, Oxford 2014) 145.

[19] This principle has been described as primary as it 'embraces and generates the other principles. It basically require data controllers to use individuals personal information in a lawful manner – i.e., a manner which takes into consideration their human right especially the right to privacy. See Bygrave (n 18)146.

[20] Basically, proportionality entail balancing conflicting interests in information processing. The interest may be the interest of data subjects vis-à-vis data controllers; data privacy rights and national security requirements etc,

[21] This principle stipulates that data controllers must adopt a minimalist approach in collecting personal information which means the personal information to be collected must be limited to that which is necessary for the stated/declared purpose. See Bygrave (n 18)151.

[22] This principle entails that personal information must only be collected for specified and lawful purpose and must not be used in a way contrary to that purpose. See Bygrave (n 18) 153.

[23] The data subject influence principle provides that data subject should be able to exert some form of influence over the processing of information relating to them. See Bygrave 158

[24] This principle requires that only the highest quality of personal data should be collected. The implication of this is that the data to be collected for the specified purpose must be valid, complete and relevant. Bygrave (n 18) 163.

[25] This principle places an obligation on data controllers to ensure that adequate security measure is put in place to check against unauthorized access to personal information which is lawfully in their possession. Bygrave (n 18) 164.

[26] This principle seeks to ensure that the processing of some category of information which are termed sensitive are given extra protection and are processes under more stringent control. Bygrave (n 18)165.

the *right of access to data which has been collected concerning* him or her, and the right to have it rectified. [emphasis added]

Compliance with these rules shall be subject to control by an independent authority.[27]

All the above data privacy norms can be found in an array of sources comprising of international treaties, decisions and recommendations of treaty bodies, domestic legislation, case law and opinions and recommendations of data protection authorities/bodies.[28] Of contemporary importance is the 'recent turn in data privacy governance towards soft law [such as code of practice] and [other] specific legal instruments [such as consumer protection and employment laws].'[29] As rightly observed, data privacy norms may be in the form of non-binding instruments which do not necessarily originate from the traditional lawmaking structure of a state but the private sector.[30] Among these sources, there is a need for further remarks on the status of data privacy as a customary norm under international law.

2.2. Crystallisation of data privacy into a norm of customary international law?

The issue regarding whether the *sui generis* right to data privacy is recognized as a binding legal concept under public international law has also generated interesting debate.[31] Since the separatists[32] have argued that data privacy should not be considered as an aspect of privacy, there is the need to interrogate its status as an international law norm. More interesting to this debate is whether data privacy has crystallized into a norm of customary international law. The implication of data privacy being considered as a customary norm under international law is that it creates an obligation towards all states, including member states of the AU, regardless of whether or not they have signed and ratified any data privacy treaty or even domesticated these norms in their local legislation. Therefore, in this regard, data privacy norms will apply to African states regardless of the status of their legal system regarding the norms.

While some scholars like Christopher Kuner denies that data privacy has indeed crystallised into a norm in international law, others argue to the contrary.[33] The most forceful voice in

---

[27] See the Charter of Fundamental Rights of the European Union (2000/C 364/01) available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf accessed 31 October 2020.

[28] Bygrave (n 18)18-19. Examples of these data protection authorities include the current European Data Protection Board based on the EU Data Protection Regulation and the former Article 29 Working Party based on the EU Data Protection Directive.

[29] de Hert & Papakonstantinou (n 2)293.

[30] Ibid. A very potent source of data privacy norm is code of conduct which could emanate from the organised private sector or group of professional bodies. Most data privacy law gives powers to groups to issue codes of conducts for the protection of personal information. For example, see chapter 7 of the South African Protection of Personal Information Act.

[31] C Kuner, 'An international legal framework for data protection: Issues and prospects' (2009) 25 Computer Law and Security Review 307-317.

[32] The separatists are a group of scholars who have vehemently argued that data protection and privacy are separate rights. Examples are P de Hert and S Gutwirth 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action' in S Gutwirth *et al* (eds) Reinventing Data Protection? (Springer, Dordrecht 2009) 8; Lynskey (n 9) 569-597; J Kokott & C Sobotta 'The distinction between privacy and data privacy in the jurisprudence of the CJEU and EctHR' (2013) 3(4) International Data Privacy Law 222-228.

[33] C Kuner (n 31)307-317.

this regard is Monika Zalnieriute.[34] Using the recent Edward Snowden's revelations of the magnitude of extraterritorial mass surveillance programs across the globe, Zalnieriute considered whether that 'international constitutional moment' has indeed occurred for data privacy to be considered as a norm of customary international law.[35] Therefore, with the aid of both the traditional and modern approaches to the formation of customary international law, she probed further into whether data privacy may indeed be considered a customary norm.[36] From the analysis of the scholar, she concluded that the status of data privacy may be doubtful under the traditional approach. But from the modernist perspective, data privacy has indeed developed into a customary norm under international law. This is especially true considering the steady advances in technology together with the increasing emphasis on international security and the common response by state governments.[37]

The debate regarding whether or not the right to data privacy has indeed crystallized into a norm of customary international law is an ongoing one. One can only hope that the UN will put this debate to rest by a more explicit statement/action. Before that time comes, it is noteworthy that data privacy norms are ascertainable in one form or the other in Africa especially with the AU Data Protection Convention. As it is usually contended by international law scholars' treaties seem to have some advantages over and above customs.[38] Apart from the clarity they come with, treaties are more orderly and develop more rapidly.[39] The next part will consider the AU treaty on data protection.

2.3. The data privacy standard of the AU: The AU Data Protection Convention

Barring all controversies concerning the evolution of data privacy as a norm of customary international law, there are still some other sources that constitute the normative framework on data privacy in Africa. Generally, apart from international law (including instruments of sub-regional bodies), national legislation, judicial decision and decisions/opinion of DPAs constitute important sources of data privacy norms. While several African states have data privacy legislation, the jurisprudence based on case law and the decisions/recommendation of DPAs is highly underdeveloped. In all, however, the AU Convention is the most comprehensive and authoritative regional-wide normative framework for data privacy in Africa. The Convention has the potentials to become the common standard for data privacy on the African continent. Perhaps that is why it has been described as 'potentially [the] most

[34] M Zalnieriute, 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) 23 International Journal of Law and Information Technology 99-133.
[35] Ibid.
[36] The traditional approach is based on an analysis of the provision of Articles 38(1) of the Statue of International Court of Justice (ICJ) which stipulates the process of formation of customary international law. In this regard, emphasis is placed on the combination of two elements in the formation of a rule of customary international law which are: state practice and the assumption of such practice as law (*opinio juris)*. The modern approach on the other hand, which emerged due to criticisms of the traditional approach, focuses on one of the elements, i.e *opinio juris*.
[37] Zalnieriute (n 34) 103.
[38] Malcom Shaw, *International Law* (6th edn CUP, Cambridge) 74. Arguing that there are some disagreements as to the value of customs as a source of contemporary source of international law.
[39] See UO Umozurike, *Introduction to international law* (Spectrum, Ibadan 2005) 19, arguing that 'codification has the advantage of clarifying doubts and minimizing disputes'

important development [concerning data privacy] in Africa'.[40] This is so for several reasons part of which includes its careful incorporation of most of the principles on data privacy which are contained in most of the international legal framework on data privacy as enumerated in section 2.1 above in this paper. Indeed, Greenleaf considers the convention to contain "relatively high data protection standards."[41]

However, as earlier noted, the Convention is yet to enter into force which means it does not create any legal obligation on member states of the AU. Article 36 of the Convention provides that the convention only comes into force after 15 states of the AU have ratified. This is yet to be achieved. There is nonetheless some sort of obligation created for states that have signed (and/or ratified) the convention even before it enters into force. According to Article 18(a) of the VCLT, such states are 'obliged to refrain from acts which would defeat the object and purpose of [the] treaty.'

Apart from the AU Convention, sub-regional bodies within Africa have also established some sort of data privacy regimes.[42] The most notable among them is the ECOWAS Supplementary Act which creates legally binding obligations on member states by virtue of its annexation to the ECOWAS Treaty.[43]

From the analysis above, it is clear that there is as yet no binding regional-wide normative framework on data privacy since the AU Convention is yet to come into force. Apart from the 'controversial' customs and probably the 'non-binding' UN instruments (and initiatives), there is no authoritative source of data privacy under international law. This, as will be argued shortly, constitutes part of the dilemma of the AU in advancing compliance with data privacy norms. The next part will scrutinize this issue more closely.

3. The African Union and the dilemma of state compliance with data privacy norms

As shown in the previous section, the AU data protection convention together with the relevant international law standard now constitutes the normative framework for data privacy in Africa. The basic principles of data privacy and other rules to enhance individuals' control over their personal information are the main norms that constitute a data privacy regime. As an international human right, the role of the AU towards promoting compliance cannot be overemphasized. It is important to state that eliciting compliance with human rights generally is usually a challenge. Hathaway rightly puts it that

> Unlike the public international law of money, there are no "competitive market forces" that press for compliance. And, unlike in the case of trade agreements, the cost of retaliatory noncompliance are[sic] low to non-existent, because a nation's actions

[40] G Greenleaf and M Georges 'The African Union's Data Protection Convention: A Major Step Toward Global Consistency?' (2014) 131 Privacy Laws & Business International Report 18–21.
[41] See G Greenleaf, 'Global data privacy laws 2017: 120 national data privacy laws including Indonesia and turkey' (2017) 145 Privacy Laws & Business International Report 5.
[42] Discussions on the initiatives of these RECs is outside the scope of this work. For more in-depth analysis, see, AB Makulilo, 'Myths and reality of harmonization of data privacy policies in Africa' (2015) 31(1) Computer Law and Security Review 78-89. See also G Greenleaf and M Georges, 'African regional privacy instruments: Their effects on harmonization' (2014) 132 Privacy Law And Business International Report 19-21.
[43] Article 48 of the Supplementary Act.

> against its own citizens do no directly threaten or harm other states. Human rights law thus stands out as an area of international law in which countries have little incentive to police noncompliance with treaties or norms.[44]

In this section of the paper, a brief analysis will be carried out on the possible challenges the AU may face in eliciting compliance with data privacy norms. This discussion is significant because most of the literature on the subject matter especially in Africa merely restates the need for countries to adopt some form of data privacy standard without a corresponding discussion on what added-value a regional body can make. Therefore, some explanation on why the AU is yet to play a significant role concerning compliance with data privacy norms is not out of place. But before this discussion, it is important to deconstruct the concept of compliance within the context of international data privacy law.

3.1. Deconstructing 'compliance' within the context of international data privacy law

Measuring the extent of compliance with an international norm has always been problematic since there are no settled principles that developed to determine *full* compliance.[45] Indeed, it may even be difficult to determine the extent of compliance without recourse to empirical data. Be that as it may, there are some general indices to determine compliance with international standards as stated by scholars. According to Viljoen, the term 'compliance' encompasses both implementation and enforcement.[46] Raustiala and Slaughter contend that 'implementation is typically a critical step toward compliance, but compliance can occur without implementation.'[47] Implementation is the process of putting international commitments in practice and it includes legislative enactment or incorporation, the establishment of institutions and the enforcement of rules.[48] International treaties will always explicitly require state parties to "*adopt legislative* or other measures to give effect to them."[49] This aspect of compliance can be easier to ascertain. The aspect of compliance which may be a bit difficult to ascertain is the extent to which the international standard induces a change in behaviour for compliance involves more than the domestic incorporation of a specific international norm.[50] In other words, compliance involves more than 'law on the books'. This introduces the concept of 'effectiveness' into the discourse on compliance as

---

[44] OA Hathaway, 'Do Human Rights Treaties Make a Difference?' (2002) 111 Yale Law Journal 1938.

[45] AT Guzman, 'A Compliance Based Theory Of International Law'(2002) 90(6) California Law Review 1823 arguing that 'international law scholarship lacks a satisfactory of why and when states comply with international law.'

[46] F Viljoen, *International Human Rights Law in* Africa (OUP, Oxford 2012) 34. VO Ayeni, *The Impact of the African Charter and the Maputo Protocol in Selected African States* (PULP, Pretoria) 1.

[47] For example, where a state is already in compliance even before the international obligation. See K Raustiala and M Slaughter, 'International law, International Relations and Compliance' in W Carlsnaes *et al* (eds), *Handbook of International Relations* (Sage London, 2002) 539,

[48] Ibid.

[49] See Art 1. ACHPR, see also article 62 of the ACHPR which provides that 'Each State Party shall undertake to submit every two years, from the date the present Charter comes into force, a report on the legislative or other measures taken, with a view to giving effect to the rights and freedoms recognised and guaranteed by the present Charter.'

[50] A Alkoby, 'Theories of compliance with international law and the challenge of cultural difference'(2008) 4(1) Journal of International law and International Relation 153 'arguing that, for example, compliance with certain environmental law and intellectual property standard will require more than mere domestication of such as standard.

there may be a high level of compliance without effectiveness and *vice versa*.[51] Nevertheless, it has been rightly stated that:

> One of the most explicit and accurate predictors of the effectiveness of an international human rights regime is the extent to which the treaty has influenced policymaking, legislative action, court decision and civil society activities at the domestic level.[52]

In more concrete terms, 'effectiveness' of a norm resulting from compliance will involve the much more complicated 'detailed analysis of the actual availability of remedies to individuals, national case-law and so on.'[53]

With regard to data privacy, after compliance usually signaled by the enactment of a data privacy legislation that contains all the basic data privacy norms, adopting the necessary legislation must also be accompanied by the institutional structure to oversee the implementation and enforcement of such norms. This is especially true for data privacy norms. Thus, the adoption of a legislation must be accompanied by the establishment of an institution - a data protection authority (DPA) - to oversee the implementation of the norms prescribed in the legislation. According to Lee Bygrave, 'DPAs frequently play a lead role in laying down how data privacy law is understood and applied, even in contexts where their views on point are only advisory.'[54] Asides from these basic measures, states must also ensure that the DPA is provided an enabling environment within which to carry out its functions. This is also in addition to the state ensuring that it does not do anything itself to undermine the international norms. Since the adoption of the convention in 2014, just about 14 of the 55 member states have signed and 8 have ratified.[55] Currently, about 23 have data privacy legislation in place. Of this 23, just 10 have established some form of an institutional mechanism to oversee the enforcement of the law. While some countries have even enacted data protection legislation and have even established a DPA, the law itself is yet to come into force. Some very influential countries of the AU have neither enacted a data protection legislation or established the relevant institutional body. This is for example the case with Nigeria.

To measure compliance by the extent of 'availability of remedies to individuals, national case-law, and so on' as stated above is much more complex. This is even so for data privacy norms in Africa considering the absence of adequate information on state practice. In Europe for example, the European Union Fundamental Rights Agency has carried out a study on Access to data protection remedies in the EU Member States.[56] The result of this study, which has

---

[51] Raustiala & Slaughter (n 47) 539. Effectiveness has been explained as the extent to which a treaty induces a change in behaviour in furtherance of the treaty's objectives.

[52] Ayeni (n 46) 1.

[53] Zalnieriute (n 34) 119.

[54] Bygrave (n 18) 4.

[55] https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf accessed 31 October 2020. Although, scholars have consistently argued that ratification in itself does not make any difference for compliance with international norms. Hathaway (n 44) 1935.

[56] *Access to data protection remedies in the EU Member states* fra.europa.eu/sites/default/files/fra-2014-access-data-protection-remedies_en.pdf accessed 31 October 2020.

been rightly described as 'the only report of its kind', is easily accessible online.[57] According to Monika Zalnieriute,

> Outside the EU, no international organization dealing with data privacy (neither the Council of Europe, Organization for Economic Co-operation and Development, Asia-Pacific Economic Cooperation, not UN) has so far compiled any database or information on the existence and effectiveness of national laws.[58]

While about 23 African countries have enacted data privacy legislation, it is difficult to determine the extent to which remedies have been used by individuals in member states. In what appears to be the most comprehensive study on data privacy in Africa – *African Data Privacy Law* – there are so little documented cases where individuals have approached DPAs or courts from remedies resulting from a violation of their right to data privacy. This is so for even countries with specific data privacy legislation.[59] Most of the cases reported have to do with the right to privacy. Only in Mauritius was it reported that formal complaints were made resulting in formal findings by the Data Protection Commissioner (the equivalent of DPA in Mauritius).[60] This is why Makulilo rightly notes that '[data]privacy is still an evolving concept in Mauritius. Nevertheless, Mauritius takes lead as far as enforcement of data protection legislation [in Africa] is concerned.'[61]

3.2. AU and the challenge of a normative framework on data privacy

The importance of a normative framework to the overall effort of an international organisation to advancing compliance with an international norm cannot be overemphasized. Indeed, according to the normative theory of state compliance with international norms, the normative force of a threat could inspire compliance or create a sought of 'compliance-pull'. Where the norms are scattered and fragmented, it will not be easy for the course of compliance to be advanced by the AU. As noted earlier, the AU convention, which is the primary source of data privacy norm of the AU, is yet to come into force although it was adopted almost five years ago. The Convention has still not obtained the number of ratifications required to come into force. There is no way the AU can advance compliance without an instrument which creates a binding obligation on member states. It is worth re-echoing that the AU as an intergovernmental institution cannot compel member states to sign or ratify treaties. According to Udombana however, the ratification of the AU Constitutive Act[62] by member states implies that 'they recognize the legal order of the AU'.[63] Such recognition, according to him, 'introduces the AU law into a field previously governed exclusively by municipal law.'[64] In a way, this implies an obligation on member states to ratify

[57] Zalnieriute (n 34) 119.
[58] Ibid.
[59] Tunisia, Senegal and Morocco.
[60] See AB Makulilo, 'Data protection in the Indian Ocean Islands: Mauritius, Seychelles, Madagascar' in AB Makulilo (ed) *African Data Privacy Laws* 289.
[61] Ibid, 290
[62] Constitutive Act of the African Union 2000. https://au.int/sites/default/files/pages/34873-file-constitutiveact_en.pdf accessed 31 October 2020.
[63] NJ Ndombaba, 'The institutional structure of the African Union: A legal Analysis' (2002) 33(1) California Western International Law Journal 129
[64] Ibid.

AU treaties in recognition of its legal order especially treaties that they did not express any reservations about.

There is the need to interrogate further on the (possible) reasons why states are yet to ratify AU Convention - for it is not enough to merely state that states have not ratified without giving some explanation as to why. Understanding these issues is complex and in a way goes to the heart of the problem the AU faces in treaty ratifications generally. In a very comprehensive study by Tiyanjana Maluwa, some of the challenges of the AU in advancing its policy goals via treaty ratification (and compliance) were analysed.[65] After considering several subject areas, he argued that there is a generally slow pace of treaty ratification by member states of the AU although, it is still better under the AU compared to the hitherto OAU. As rightly observed, 'no matter how admirable the AU's policy goals and objectives on any issues address by a treaty may be, the treaty is nothing more than an expression of the member states' aspirations until it is ratified and becomes binding.'[66] However, Maluwa identified human rights as one of the areas where treaty ratification has been relatively faster! A general conclusion reached by the author at the end of his analysis which directly impacts data privacy is

> …that treaties that do not create any tension with the domestic legal regime and structure and only require minimal changes to existing national law, stand a better chance of getting ratified.[67]

As was observed earlier, data privacy is one such area where the legislators must do more. As part of the requirement of international data privacy law, there is the need to first enact legislation which should contain all the principles of data protection. As if to make matter worse, there is also the requirement to establish an institutional framework to oversee the implementation of the law. This naturally has some financial implication which African states will be reluctant to bear considering that data privacy may not be considered as part of the 'hot' priority areas where African leaders can easily score cheap political points. Besides, the technicalities which data privacy law entails will require the need for some sort of expertise in the making of the law. For example, the South African Law Reform Commission commissioned an expert group in the process of drafting the South African Protection of Personal Information Act which took about 10 years to complete.[68] Indeed, not every African state will (easily) want to be bound by an obligation to commit such huge resources.

Another possible explanation of why African states are yet to ratify the AU Convention which impacts on the AU's ability to induce compliance is the perceived weak conception of privacy-related issues in the continent. Based on this theory, African states are collectivists in nature while Western societies are individualistic. Collectivism denotes that individuals in a community do not operate individualistically as an entity without the consent of their family,

[65] T Maluwa, 'Ratification of African Union treaties by member states: law, policy and practice' (2012) Melbourne Journal of International Law 1

[66] Ibid 5.

[67] Ibid.

[68] See generally SALRC Project 124, *Privacy and data protection report* 2009. Available at http://salawreform.justice.gov.za/reports/r_prj124_privacy%20and%20data%20protection2009.pdf accessed 31 October 2020.

clan or tribe.[69] In this regard, the concept of privacy is antithetical to a collectivist structure which is largely associated with the culture in Africa.[70] This argument has been stated to be a reason why the ACHPR did not include the right to privacy. According to Heyns, this is one of the latent shortcomings of the charter. [71] Despite a growing movement toward a 'separationist' approach wherein the right to data privacy is considered as separate from privacy, one cannot easily divorce data privacy from its roots. Africa is yet to get to that 'separationist' point as even the Data Protection Convention provides the protection of 'privacy' as one of its main objectives.[72]

Other issues that speak to the low level of ratification of the Convention include the low level of awareness by policymakers and the people of the threats resulting from the unregulated collection and use of individuals' personal information. Malula's remark is apt in this regard where he observed that

> Treaty ratification campaigns undertaken by some non-governmental organisations in Africa have sometimes revealed that legislatures may be reluctant to ratify a treaty due to misconceptions, or a lack of appreciation of the legal and political import of the treaty, arising from the failure or inability of the bureaucrats in the relevant government department to provide the necessary technical advice.[73]

There are still other significant normative challenges which the AU may face in advancing the course of data privacy on the continent. The absence of a fundamental basis for data privacy in the AU legal regime is a notable problem with several implications. As earlier noted, the ACHPR is the only international human rights treaty in its category which does not recognize a right to privacy. This means data privacy norms will struggle to find a firm footing in the AU's jurisprudence. Even when the convention comes into force, it will not be possible to link it to any fundamental human right guaranteed under the key regional human rights instrument - ACHPR. It is rather surprising that the AU Convention in its preamble refers to the need to establish a regulatory framework on data protection which takes into account the requirement to respect fundamental rights of citizens under fundamental texts and domestic law *particularly the ACHPR*. One wonders which of the rights in the ACHPR the convention refers to. In sharp contrast, the EU Data Protection Directive for example makes the realisation of the right to privacy as provided in the Treaty on the Functioning of the European Union (TFEU) a core value.[74] Similarly, the General Data Protection Regulation (GDPR) also provides that the right to protection of personal data is a core value.[75] In this way, there is a linkage between the GDPR and the EU Charter which provides for the right to data protection.

---

[69] AB Makulilo, ' "A Person Is a Person through Other Persons"—A Critical Analysis of Privacy and Culture in Africa' (2016) 7 Beijing Law Review 194.

[70] HN Olinger *et al*, 'Western privacy and/or Ubuntu? Some Critical Comments on the influences in the Forthcoming Data Privacy Bill in South Africa' (2007) 39(1) The International Information & Library Review 31.

[71] See CH Heyns, 'The African Regional Human Rights System: The African Charter' (2003) 108 Pennslyvania State Law Review 687

[72] See Article 8(2).

[73] Maluwa (n 65)34.

[74] Consolidated Version of the Treaty on the Functioning of the European Union https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN accessed 31 October 2020.

[75] See art 2.

Related to the above is the fact that data privacy has so far not really been considered by the AU, Regional Economic Communities (RECs) and state parties as a human right.[76] Due to its dual but conflicting objectives (economic/human rights), the economic perspective seems to prevail on the continent. For example, the inclusion of data protection norms among other economic-related instruments in the Convention is a justification of this fact. The AU Convention covers three broad areas in one treaty – electronic transaction, data protection and cybersecurity. Even the state parties to the convention note that a major obstacle to electronic commerce in Africa is related to issues covered by the convention. This paints a clear picture of the rationale for the convention. Unlike in Europe where data privacy was initially advanced for economic motives, the current jurisprudence has shown a paradigm shift to the human rights objectives in line with the recently expanded mandate of the EU bothering on human rights. As will be consistently argued, data privacy is a human right that should be given its place in the human rights system of any region. The AU will continue to face significant challenges if it does not include data privacy as part of its human right work in the continent. Besides, it has been rightly noted that the rate of ratification of human rights treaties is higher in the AU than in other subject areas.[77] It is therefore arguable that the AU and member states take the human rights agenda more seriously.

It is also arguable that the general perception of the objectives of data privacy in Africa and among African states is that which has to do with enhancing commerce. Makulilo rightly observes in this regard that

> As far as the African countries are concerned, in most cases securing better chances for off-shoring business from Europe is a major reason as to why African countries have adopted or plan to adopt comprehensive data protection laws.[78]

This has therefore made the AU (and other regional bodies such as the RECs) less influential in data privacy issues. African states will prefer to 'copy' the European norms rather than develop and advance a truly African data privacy normative framework. For example, three African Countries (Morocco, Cape Verde and Burkina Faso) have requested to be invited to accede to the CoE Convention when they have neither signed nor ratified the AU Convention.[79] It is noteworthy this attitude comes with a cost. As was rightly noted by some scholars that the EU standards is by no means a panacea and 'it builds upon and reflects European state organisation concepts that may not be suitable to all countries around the

[76] There are 8 RECs in Africa based on the 1991 Abuja treaty which establishes the African Economic Community. They are Arab Maghreb Union (AMU) in north Africa; Economic Community of West African States (ECOWAS); East African Community (EAC); Intergovernmental Authority on Development (IGAD); Southern African Development Community (SADC); Common Market for Eastern and Southern Africa (COMESA); Economic Community of Central African States (ECCAS) and Community of Sahel-Saharan States (CENSAD). See https://www.un.org/en/africa/osaa/peace/recs.shtml accessed 31 October 2020. So far, only ECOWAS, EAC, IGAD and SADC have been active in the subject of data privacy protection.

[77] Maluwa (n 65) 20.

[78] de Hert & Papakonstantinou(n 2) 19.

[79] G Greenleaf, 'The UN should adopt Data Protection Convention 108 as a global treaty..' https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf accessed 31 October 2020.

globe.'[80] Some of the criticisms against the EU standard is its highly rigid nature. Rigidity has often been associated with the bureaucracy involved, the complexity of provisions making it difficult for compliance and the high sanction/cost for non-compliance. For Africans, who are only new to data privacy issues, there is the need to take gradual steps to make compliance easier and to entrench the norms. All these have made any truly African initiative towards advancing data privacy in the continent very challenging.

3.3. AU and it's institutional (and other) challenge

Apart from the challenge and uncertainties brought about by the AU normative framework on data privacy, there are also some general institutional challenges which may impact on its ability to induce compliance with data privacy norms. These challenges have to do with the general problem of the AU and its competence to influence members to not only sign, ratify and domesticate AU treaties, but to comply with their treaty obligations. This is a much deeper and complex challenge which includes issues such as the ability of the AU to develop innovative means to deal with the general absence of political will by African leaders in crucial issues and the size of the African region. Indeed, the sheer geographical size and the size of its members are facts which impact on the management of the Union and may arguably affect the work of the AU.[81] The implication of this vast geographical space is a challenge in norms diffusion.[82] Other complex challenges the AU faces, which are institutional, include financial issues[83] and its weakness in terms of enforcement of sanctions generally. It is also noteworthy that there are growing concerns that the AU now focuses so much on 'international development cooperation and relationship with international partners' at the detriment of its member states' interests.[84] As important as these institutional challenges are, this paper will not dwell so much on them for two reasons. First, they are issues that have been extensively dealt with in other literature and second, most of them are challenges that are not strictly legal and therefore beyond the scope of the current exercise.

4. Making the AU effective in advancing compliance with data privacy norms: Lessons from the European data privacy system

The preceding section has shown that when it comes to promoting compliance with data privacy norms, the AU has played a weaker role compared to its counterparts in other parts

[80] de Hert & Papakonstantinou (n 2) 314 'according to the scholar, the EU data protection approach refers to a rigid and structured data protection model that may appeal to organized (mostly Western-style) bureaucracies, but may deter newcomers in the field, particularly emerging economies that may see some benefit in adopting a more flexible and relaxed solution.' See de Hert & Papakonstantinou (n 2) 315.

[81] For example, unlike the EU which has a total of 26 economically viable countries, the AU comprises of 55 developing countries.

[82] O Babarinde, 'The EU as a Model for the African Union: the Limits of Imitation' http://aei.pitt.edu/8185/1/BabarindeEUasModellong07edi.pdf accessed 31 October 2020.

[83] See S Elvy, 'Theories of state compliance with international law: Assessing the African Union's ability to ensure state compliance with the African Charter and Constitutive Act' (2012) 41 Georgia Journal of International & Comparative Law 90; See also 'Main successes of the AU in peace and security, challenges and mitigation measures in place' https://au.int/fr/pressreleases/20170127/main-successes-au-peace-and-security-challenges-and-mitigation-measures-place accessed 31 October 2020. where it was rightly observed that lack of funds is a huge challenge facing the AU.

[84] See F Lisk, 'The African Union after 10 years: Successes and challenges' https://warwick.ac.uk/newsandevents/expertcomment/the_african_union/ accessed 31 October 2020.

of the world. It is therefore no surprise that compliance is comparatively lower in the continent. In this section, a brief analysis will be carried out on means to strengthen the AU towards advancing compliance with data privacy norms. For the analysis, it is important to explain, in brief, the sense in the use of the term 'strengthening' or 'giving teeth'. In this paper, both terms are given a wider connotation to mean making the AU more 'influential' and 'active' in the field of international data privacy generally and promoting the implementation and enforcement of data privacy norms specifically. This, as will be seen shortly, entails a combination of measures which go beyond mere coercive or forceful mechanisms for 'the AU lacks powers to compel member states to ratify its treaties and comply with their provisions'.[85]

4.1. Why AU?

There are at least four reasons why the AU needs to play a more active role in the subject matter. (a)In line with the widely acknowledged advantages of regional arrangements, in promoting international human rights norms generally. Indeed, according to Viljoen,

> The relative advantage of the sub-regional and regional levels, compared to the global level, is the higher level of convergence and coherence between states, allowing for greater norm-specification in the regional and sub-regional spheres; and the immediacy of interlocking interests, opening the possibility for faster response and improved implementation when states are closely bound by economic and political ties.[86]

(b) Related to the above is the fact that since there is significant pessimism as to the possibility of the emergence of a truly globally binding data privacy standard and monitoring institution, regional arrangement to advance initiatives in this increasingly critical area of law is not out of place.[87] Scholars have made specific arguments regarding why the UN cannot occupy the position of a global data privacy institution.[88] Apart from the intense power tussle between the most politically influential member states on the best means to realize data privacy, the UN 'kept clear from the data privacy field after the release of its Guidelines in 1990.'[89] (c)

---

[85] Maluwa (n 65) 1.

[86] Viljoen (n 46) 9.

[87] See discussions by Kuner (n 31) 307-317. According to the scholar,

> '*The time does not yet seem ripe for a binding international legal instrument on data protection*: the difficulty of selecting the standards that should serve as the basis for a binding legal instrument, of agreeing on its scope, and of selecting an appropriate international organization to coordinate the work, indicates that the drafting of such an instrument is unlikely to be possible within a reasonable time period, and to a useful degree of specificity'

Since 2009 when the view above was expressed, one wonders if anything has changed (or is likely to change) 10 years after considering the increasing attention that is been paid to the topic of human rights in the digital age by the UN. Nevertheless, in 2013, the same author expressed similar sentiment when he argues that 'The best view seems to be that data protection is an "emerging" fundamental right that has not yet gained full recognition under public international law, but may do so in the future.' See C Kuner, 'Extraterritoriality and the fundamental right to data protection' (2013) EJIL: Talk! https://www.ejiltalk.org/extraterritoriality-and-the-fundamental-right-to-data-protection/ accessed 31 October 2020.

[88] Christopher Kuner, 'The European Union and the search for an international data protection framework' (2015) 2(1) *Groningen Journal of International Law* 56. Arguing that the Guidelines have had very little impact.

[89] de Hert & Papakonstantinou (n 2)288. The authors were however of the view that the UN still has the capacity to be the global data privacy governance institution.

Besides, the UN Guidelines on data privacy[90] which is a product of the only truly global institution - the UN - has been criticized by scholars as not capable of occupying the position of a global standard on data privacy. Lee Bygrave for example contends that the 'soft law' status and its 'greater stringency' on key issue have made it less influential.[91] Its soft law or non-binding status has however been stated not to be a credible reason why the UNs instrument is not as influential considering how significant the OECD Guidelines is in this regard.[92]

(d) Furthermore, a more active AU will make norm specification and prescription easier thereby facilitating internationalisation and standardization of data privacy norms for Africa. Indeed, a stronger regional system for data privacy will enable more convergence of states towards harmonisation and unification of data privacy norms. From this perspective, the AU being the foremost regional body will be able to more effectively coordinate not only the activities of states on the subject matter but the initiatives of the highly dispersed RECs who have also ventured into the field. Indeed, all these are possible since all African countries are member states of the AU.[93]

4.2. Giving real effect to the AU in advancing data privacy norms compliance

Returning to the question of how the AU can be strengthened towards advancing compliance with data privacy norms in African countries,[94] we find the theories of compliance with international norms relevant. The realist theory of compliance with international law postulates that states sometimes comply not because of genuine interest in complying but for sanction or fear of sanction by other states or international organisations. Nevertheless, it has been argued that 'international legal norms only become truly effective if compliance is not motivated by coercion or self-interest but flow from personal motivation brought about by an internal process of norm-acceptance'.[95] The question then is how can the AU be more effective in promoting that 'internal process of norm-acceptance' concerning data privacy. Considering the general problem of African states and their sloppy attitude towards international treaties, there is the need for a 'superior' institution to sometimes prod them into compliance. In this regard, we still find answers in the theories of compliance with international norms, particularly the normative and institutional theories. The rest of the

[90] Guidelines Concerning Computerized Personal Data File (UN General Assembly Resolution 45/95) 14 December 1990.

[91] Bygrave (n 18) 53.

[92] Ibid.

[93] Morocco was the only African state that was not a member but it was re-admitted in early 2017. Morocco left the previous Organisation of African Unity (OAU) in 1984 after it recognised the independence of Western Saharan which Morocco has considered to be part of its territory. In 2017 after intense lobbying, it was re-admitted to the AU. 'Morocco to rejoin African Union despite Western Sahara dispute' https://www.bbc.com/news/world-africa-38795676#:~:text=Morocco%20has%20been%20readmitted%20as,part%20of%20its%20historic%20territory accessed 31 October 2020.

[94] According to Viljoen, enforcement and implementation constitutes compliance. He argues further that enforcement takes place when a provision of international law is applied as a basis for a remedy under national law or when international norms reach individuals in member states while implementation refers to giving effect to an international treaty provision and pronouncement by treaty bodies in domestic policies and legislation. Viljoen (n 46)34.

[95] Viljoen (n 46) 25.

section will attempt an explanation, using both theories, of how the AU can be more effective in prodding states into compliance with data privacy norms.

In summary, the institutional theory focuses on the role and power of international institutions in changing state behaviour and facilitating cooperation. Unlike the realist theory, the institutional theory looks into how a state can avoid 'cheating' and genuinely comply with international norms with the assistance of international institutions.[96] Membership of an international arrangement positively impacts states by creating an incentive towards compliance with international norms.[97] Of particular importance according to the institutionalist is the fact that mere membership of an international organisation is not enough to ensure compliance. The institutional strength and willingness to prod states towards enforcement and implementation will have a significant bearing on the compliance by individual states.[98] The normative theory on the other hand looks to the normative force of a treaty or an international norm to induce compliance. In this regard, the extent of inclusiveness in the norm creation, transparency and credibility in the system of implementation are all factors that enhance compliance. According to Hathaway, the theory relies strongly on the 'persuasive powers of legitimate treaty obligations.'[99]

One of the key contributions of the normative theory in the discourse on compliance with international norms/obligations is the significance of persuasion (and conviction) which could be brought by (continuous) dialogue on a subject matter. According to Hathaway, a fundamental claim by the proponents of the normative theories is that 'it is the transformative power of normative discourse and repeated interactions…that is responsible for the formation and continuation of human rights regime.'[100] In this regard, there is an urgent need for an organisation of serious dialogue on the threats associated with data privacy and the need for compliance with its norms. This dialogue should be anchored by the AU with the support African Union Commission. The role of civil society organisations such as Article 19 and Privacy International is also paramount to this project. This dialogue should not merely be a once-off thing but should be continuous in the light of the normative theory which requires 'repeated interactions' for norm diffusion. This dialogue, which could operate like the World Summit on Information Society (WSIS) forum[101], should include key stakeholders in member states such as government, civil society, private sector, academic community etc. The Agenda of this 'Africa submit' should address various issues regarding 'Africa, data privacy and human rights.' Like the WSIS Forum, the program of such a dialogue should be completely crowdsourced so that Africans can have a serious input in the project. While this may not be a magic bullet to the challenge of data privacy on the continent, it is at least, an important first step. This can indicate the seriousness of the AU in these matters.

This African dialogue can also serve another useful purpose in that it will attract attention to data privacy thereby making it take its position at the top in the agenda of the AU as it is with

[96] See C Powell, 'United States Human Rights Policy In The 21st Century in The Age Of Multilateralism' (2002) 46 Saint Louis University Law Journal 421
[97] Elvy (n 83)79
[98] Viljoen (n 46) 34.
[99] Hathaway (n 44) 1955
[100] Ibid 1957.
[101] https://www.itu.int/net4/wsis/forum/2018/ accessed 31 October 2020.

the UN and other regional bodies. As it was rightly observed by Kuner, data privacy issues are 'destined to remain one of the most important regulatory and policy issues of the 21st century'.[102] This shows that data privacy cannot be ignored at any level. The current debate regarding the mass surveillance by the US NSA and its implication on human rights and fundamental freedom is an issue which no region of the world can afford to ignore.[103] Apart from the AU in general, data privacy issues should also be part of the work of one of the Specialized Technical Committees established under Article 14 of the AU Constitutive Act.

From the institutional theory perspective, a specialized technical committee which should have data privacy as part of its mandate serves another useful value. Although the role of such a committee is merely advisory, such a committee according to Kirgis

> use a more positive compliance strategy. Quite often, the reason for a member state's noncompliance with an agency norm is not willful disobedience; rather, it is a lack of technical capacity to comply. In such cases, agencies usually try to supply technical assistance or advice. Their ability to do so depends, of course, on the extent of their financial and technical resources and the severity of the technical shortfall in the member state. If the resources are available, this can be an effective compliance device. When the circumstances call for it, the technical assistance can be combined with some persuasion to generate the will to comply as well as the technical ability to do so.[104]

As earlier noted, data privacy is one such subjects where there is an urgent need for such technical capacity. Yet still, within the AU, other structures can also take an active part in monitoring compliance like the AU Commission. Within the EU, other institutions in the organisational structure play quite a significant role in ensuring compliance with data privacy norms regardless of its longstanding and deeply entrench data privacy system. For example, the European Commission,[105] which is like the legislative and executive arm of the EU, also monitors compliance. In this regards, Paul de Hert and Vagelis Papakinstantinou stated that

> Even within the EU, the European Commission has frequently had to intervene in order to ensure compliance, even though the EU Data Protection Directive has existed for over fifteen years and Member States harmonized their legal systems accordingly.[106]

The role of another important agency of the AU cannot be ignored especially in terms of norm creation, diffusion and internationalisation. This agency is the AU Commission of International Law (AUCIL).[107] This is a very important agency of the AU which seeks to advance the objectives of the Union through promoting research in all fields. The Commission also seeks to maintain standards in important areas of international law. Data privacy can be brought

[102] C Kuner, *European data privacy law and online business* (OUP, Oxford 2003) xi.
[103] D Cole and F Fabbrini, 'Bridging the transatlantic divide? The United States, the European Union, and the Protection of Privacy Across Borders' (2016)14 I.CON 220.
[104] FL Kirgis, 'Enforcing international law' (1996) 1(1) American Society of International Law Insights https://www.asil.org/insights/volume/1/issue/1/enforcing-international-law accessed 31 October 2020.
[105] 'What the European Commission does in Law' https://ec.europa.eu/info/about-european-commission/what-european-commission-does/law_en accessed 31 October 2020.
[106] de Hert & Papakonstantinou (n 2)289
[107] (n 105).

within the agenda of the AUCIL since it also has the mandate to 'conduct studies on legal matters of interest to the Union and its member states.'[108] Another critical role of the AUCIL will help improve the level of awareness on data privacy is in the aspect of encouraging the teaching, publication and dissemination of literature on international law with particular emphasis on the AU law. An equivalent of the AUICL, albeit with a narrower mandate, is the European Union Agency for Fundamental Rights (FRA).[109] This body made significant strides in three major areas: collecting and analysing information and data, providing assistance and expertise and communicating and raising rights awareness.[110] Unlike the AUCIL, the FRA does not have a specific role concerning harmonisation and internationalisation. This is one area where the AUCIL can add value to the AU and data privacy compliance if it is active. Indeed, Stacy-Ann Elvy's remarks on the AUCIL for the institutional theory perspective is noteworthy where she contends that

> From an institutionalist perspective, a regional human rights system can obtain state compliance by clearly establishing unambiguous rules and norms for states to follow. Thus, in order to replicate the ILC's success, the AUCIL must become more active in promoting and establishing clear norms and rules for the African Union. Moreover, the AUCIL should be instrumental in creating new methods, via drafting new instruments, to better ensure member state compliance with the principles set forth in the African Charter and Constitutive Act.[111]

One apparent lapse of the AU Convention which may affect the ability of the AU to push states to comply with data privacy norms when eventually the treaty comes into force is the absence of a specific supervisory agency. The Article 29 Working Party, for example, was created by the EU under the EU Data Protection Directive. This body has been replaced under the new General Data Protection Regulation with the EU Data Protection Board. This agency, from an institutional perspective, performs a very critical role as it is a key source of data privacy norms in the EU. [112] They help interpret and granting proper guidance on the regional wide application of the norms to ensure uniformity.

Like the EU, there is a need for a more solid fundamental basis for data privacy. At least, it is now clear, despite the initial doubts, that the right to data privacy is a (fundamental) human right. In the EU according to Taylor, '[d]ata protection has noticeably been moving away from being referred to as an economic necessity to being promoted…as a fundamental right.'[113] The recognition of data privacy as (fundamental) human right under the AU system will not only make the AU take it enforcement more seriously but will create the obligation on states to respect, protect and fulfill the right. The most important step is to at least adopt a Protocol to the AU Charter containing the right to privacy since it has been established that it is an important value for Africans as well. A suggestion that a *sui generis* right to data privacy be incorporated into the ACHPR like it is in the EU Charter may sound too ambitious but feasible.

---

[108] 'About AUCIL' https://au.int/aucil/about accessed 31 October 2020.
[109] 'About FRA' https://fra.europa.eu/en/about-fra accessed 31 October 2020.
[110] 'FRA: What we do' https://fra.europa.eu/en/about-fra/what-we-do accessed 31 October 2020.
[111] Elvy(n 83) 70.
[112] de Hert & Papakonstantinou (n 2) 290-291.
[113] M Taylor, 'The EU's Human Rights Obligations in Relation to its Data Protection Laws with Extraterritorial Effect' (2015) 5(4) International Data Privacy Law 246-256.

However, a more moderate recommendation is to start with the right to privacy. In any case, even the European Convention on Human Rights (ECHR) does not contain an independent right to data privacy however, it is read into the right to privacy. The trend toward adopting independent data privacy right is however a global one. Indeed, the human rights implications of digitalisation and datafication are not just problems for the developed countries. Developing nations are also exposed to these risks as much as developed nations are. It is in recognition of this fact that a scholar opined that it is *time for a fourth generation of human rights?*[114] The fourth generation of human rights being advocated for is digital rights with data privacy given its due prominence. This is due to the very tough questions that emerging technologies pose to traditional human rights. 'Indeed, these issues are everyone's concern and require a new generation of human rights.'

The general argument that Africans' collectivist rather than individualistic culture is a reason why there is a weak notion of privacy in the continent has been successfully disproved by scholars. Besides, with globalisation, rapid advances in telecommunication and the internet on the continent, such arguments may no longer be tenable. That is why Makulilo contends that 'Under globalization African culture of collectivism has to a large extent given way to Western individualism.'[115] Moreover, such an argument may only hold some weight in privacy discourses and not data privacy. Considering the established differences between both norms and the different values they seek to promote, that 'individualism and collectivist' dichotomy is irrelevant in data privacy discourse. Africans access the internet and their personal information are also highly sought by both private and public data controllers. This is, according to some scholars, a 'common problems, which are commonly felt'.[116] It, therefore, means Africans ought to be protected using appropriate legal norms. Again, the international data privacy norms are crucial for Africa as much as it is the western world and should therefore be taken seriously.[117]

The recognition and consequent incorporation of data privacy as a core value in the AU charter will also bring data privacy within the jurisdiction of the African Commission on Human and People's Rights. This will create a legally binding obligation on state parties to 'report on the legislative or other measures taken' towards compliance with data privacy norms.[118] This also has its overall impact on the human rights regime of African states in general and will enhance compliance. Such a move is in line with the institutional theory that 'state compliance with the norms of a human rights regime will be greatest in regions where the human rights regimes are strong, for example, the EU system.'[119]

---

[114] C Soh *et al*, 'Time for a fourth generation of human rights' http://www.unrisd.org/TechAndHumanRights-Soh-et-al accessed 31 October 2020.

[115] AB Makulilo, 'The Context of data privacy in Africa' in AB Makulilo (ed) *African Data Privacy Law* (Springer, Switzerland 2016) 14.

[116] de Hert & Papakonstantinou (n 2) 319

[117] According to Nwanko 'It is admitted that Europeans may have some historical, philosophical and technological reasons for their stance on privacy, but the privacy issues we face today are more or less the same globally, especially with rapid innovations in the ICT' IS Nwanko, 'Information Privacy in Nigeria' in AB Makulilo (ed) *African Data Privacy Law* (Springer, Switzerland 2016) 52.

[118] Article 62 of the ACHPR.

[119] Elvy (n 83) 79.

In all, the institutional and normative theories give useful guidance on how to make the AU more influential and active in the field of data privacy on the continent without necessary recourse to sanctions.

5. Conclusion

Being the leading human rights institution in Africa, the AU has a serious role to play when it comes to advancing compliance with digital rights especially the right to data privacy. Indeed, the overall benefit of regional initiative cannot be overemphasized especially in terms of coordinating efforts in a highly fragmented community like Africa. Despite its structure which is different from the EU, the AU can still play a more active role with regard to the enforcement of data privacy norms especially by bringing it within their human rights works and coordinating efforts toward inducing compliance. While it is acknowledged that data privacy is still in its infancy in Africa, the argument being made in the paper is that the development of the normative framework has been rather too slow. This position is so especially when considered in the light of the rapid advances in technology and the internet on the continent. This is besides the growing penchant by African government to access private-sector information on individuals.

The AU Convention has not been so influential in advancing compliance with data privacy norms because the AU itself has been docile in the aspect of advancing digital rights generally. There is an urgent need for a paradigm shift. The first step, as was noted above, is the need for that serious dialogue heralding the threats of information technology in the digital age and the need to curtail this threat. The dialogue must all highlight how and why only the AU can effectively champion regional initiative in the subject matter. Furthermore, the dialogue must also emphasize that data privacy is no longer a right which African state seeks to fulfil so as to facilitate their access to European markets because of the demand of the EU data protection system. That is realist thinking which should have no place in human rights. African state must not only comply with data privacy norms to enhance their reputation in the international community but for the betterment of human rights and the advancement of democracy on the continent. The time is indeed now! The AU must take its proper position in these issues!