AI in Africa: regional data protection and privacy policy framework for social good

Raymond Onuoha
Lagos Business School, Pan-Atlantic University
ronuoha@lbs.edu.ng; raymondonuoha@yahoo.com
+2347039833155

1. Introduction: Problem Statement

Basking on the ubiquitous adoption of mobile technology adoption in Africa, experts in the technology domain prognose a similar upswing in the application of artificial intelligence (AI) especially in the communications space and expect it to help leapfrog critical challenges on the continent (Bostrom et al, 2018; Dafoe, 2018; Gadzala, 2018). With the predicted prevalence of significant advancements relying on artificial intelligence up till 2040 (Turianskyi, 2018), there seem yet very sparse collective attempts by regional governments in Africa and the continent as a whole at regulating the critical issues that emerge in this regard especially with regards to data protection and privacy - such as government surveillance or corporate influence over customers. Though the challenge of specific AI-related cyber policy formulation on the continent may appear unrealistic at this early stage, it is of high imperative to initiate critical discussions on the context-specific requirements with regards to adaptations of existing or formulation of new regulatory policy as it pertains to artificial intelligence. This will be critical in providing a cohesive regional-level policy roadmap for channeling the massive potential of artificial intelligence deployment on the continent especially with regards to appropriate institutional configuration for international cooperation on data protection and privacy.

Nevertheless, even with the limitations of existing data protection and privacy policy frameworks on the continent with respect to artificial intelligence developments, their adoption and effective implementation by member countries in the region is still a fundamental reference point for ensuring that critical safeguards are in place while we seek to maximize the benefits of AI deployments. The closest policy document on the continent in this regard – *African Union's 2014 Convention on Cyber Security and Personal Data Protection*[1] - currently has been signed by just eleven out of the fifty-five member countries (these include: Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mozambique, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia), while only three member countries (Guinea, Mauritius and Senegal) have ratified the policy document[2]. While the treaty provides '*fundamental principles and guidelines to ensure an effective protection of personal data and create a safe digital environment for citizens, security and privacy of individuals' data online*'[3], it makes no reference to institutional strategies of mitigating the threats posed specifically by artificial intelligence deployments on the continent.

At the sub-regional level, the focus has largely been on the policy element of data privacy, with the Economic Community of West African States (ECOWAS) leading the way via the *2010 Supplementary Act on Personal Data Protection within ECOWAS*. Similar, albeit non-binding policy instruments have also been developed by the East African Community (EAC) – *the2012 Bill of Rights for the EAC and the 2011 draft EAC Legal Framework for Cyber Laws*. In the same regard, the Southern African Development Community (SADC) established the *Model Law on Data Protection* in 2012, but has since been non-binding on member states, making implementation and enforcement difficult (Turianskyi, 2018). A similar area of disharmony especially at the regional levels includes differences in policy formulation that generally undermines levels of compliance. This situation demands more continent-level coherence for easier adoption and implementation, which if persists, inadvertently increases the gap between the frontiers of global technology and mechanisms of local and regional governance that has geopolitical ramifications for the continent (Evanoff & Roberts, 2017). To help close this gap, there is the need to research the challenges to AI-related data protection policy mechanisms of regional blocs on the continent as well as the slow adoption of the continental-level data protection framework in order to proffer evidence-based recommendations to addressing the situation. The end result will be to assess the efficacy of alternative collective approaches to data protection policy and regulation especially in relation to peculiarities of artificial intelligence in the African context. This process will help ensure that the transnational benefits of artificial intelligence deployments as they emerge on the continent work for both public and societal good, while minimizing risks. In this regard according to Makulilo (2015: 87):

> '*policymaking and regulation at the level of international union requires a correct balance between the* ***benefits*** *of the harmonisation of policies and the internalisation of* ***cross-country spillovers and the costs*** *related to heterogeneous preferences of the countries that take a decision in common'.*

Nevertheless, while compliance to regional data protection and privacy policy frameworks is important, there is also the critical need to assess their efficacy in dealing with emerging challenges posed by AI deployments on the continent, and if or what changes should be adapted in this light in a manner that will not weaken data protection itself or impede the benefits of artificial intelligence. In undertaking

[1] Accessed January 21, 2019: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
[2] Accessed January 21, 2019: https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection_1.pdf
[3] African Union Cyber Security Expert Group Terms of Reference (ToR). Accessed March 13, 2019: https://au.int/sites/default/files/announcements/34877-annc-au_cyber_security_expertgroup_tors.pdf

this process, a principle-based policy making process that aligns with the contextual nuances of the region should be taken into consideration. Therefore, based on these submissions, the key research questions that this study seeks to answer are:

1. *What are the institutional challenges of regional/continental data protection cyber policy cooperation in Africa?*
2. *What are the social benefits of regional/continental data protection cyber policy cooperation in Africa viz-a-viz cross-country spillovers and costs?*
3. *What are the AI-related social values and principles around which the sub-regional entities can coordinate in data protection cyber policy for the continent?*
4. *What are the least infringing possible institutional arrangements for a harmonized data protection cyber policy on the continent?*
5. *What adaptations of the existing regional/continental data protection policy frameworks are required to effectively deal with emerging challenges of artificial intelligence?*

The overall research objective will be to explore AI-related data protection and privacy governance at the regional (delimited to the ECOWAS sub-region) and continental level in relation to the Africa Union as countries begin to adapt to rapidly changing socio-technical environments. This will entail a deeper understanding of the policy evolution, processes and attributes of the regional entities on the continent with regards to data governance, as well as the challenges and opportunities of a multilateral approach to cyber policy formulation and adoption on the continent with respect to data protection and privacy.

2. Literature Review

2.1 Artificial Intelligence and Data Protection and Privacy Policy

The nexus between artificial intelligence and data are driven by three key change mechanisms: complex computing power, autonomous algorithms, and increased data (structured and unstructured) capture and storage from online searches, social media and connected devices (Campolo et al., 2017; OVIC, 2018). These changes are altering the traditional scope of informed consent and data access, control and processing especially in regards to identifiability, opacity and unpredictability of data outcomes, and therefore necessitating the requirements for adapting the traditional data protection and privacy policy with the current realities of artificial intelligence (Kuner et al., 2018). Data protection is important for privacy and security not just for the sake of effective regulation alone (to the extent it is essential), but also for ensuring data quality for creativity and innovation as data travels across regional borders.

2.2 Transnational cyber policy and governance

From a borderless paradigm of the Internet ecosystem, transnational data protection policy and governance seeks to regulate data capture and processing as they flow across national boundaries in order to minimize risks while maximizing opportunities derivable. Consequently, international cooperation is required in mitigating multilaterally the threats of cybersecurity and data breaches especially as they relate to artificial intelligence application (Sofaer & Goodman, 2001; Maurer, 2011; Greiman, 2018). This makes transnational institutions and organizations in collaboration with national regulatory entities as the more effective governance levers for addressing cyber policy challenges than tackling the challenges in national silos (Solum, 2009; Mussington et al., 2018).

In analyzing the institutional features of a transnational governance arrangement, detailed attribution is made to the complex interrelationship between the collaborating entities (both vertically and horizontally) with regards to competing and complementary dynamics as they co-evolve (Burke-White, 2003; Lehmkuhl, 2006). Harmonizing a coherent policy formulation for a more robust international coordination of AI-related cyber governance will require 'optimal alignment of procedu*res, policy outputs, instruments and actors, necessary to tackle security threats that are not bound by national borders'* in a manner that will not undermine transnational integration (Carrapico & Barrinha, 2017: 1257; Brattberg & Rhinard, 2012; Mattoo& Meltzer, 2018).

2.3 ECOWAS Data Protection Convention in the context of other regional data protection frameworks

The ECOWAS 2010 *Supplementary Act on Personal Data Protection* comprises critical data protection provisions and exceptions such as data access rights, compulsory data processing declaration, sensitive data authorization as well as personal data processing guiding principles. However, in contrast to some other regional data protection frameworks on the globe such as the more recent European *General Data Protection Regulation(GDPR)*[4] and to some extent the OECD[5] privacy guidelines[6], key data protection principles with significant imperatives for artificial intelligence developments within the region are missing, such as those for data security breach notification especially for automated decision-making, data portability, minimization (especially the right not to be subjected to automated decision-making) and the *right to be forgotten*; as well as some privacy omissions with regards to data privacy by design and/or by default obligations especially in relation to purpose specification (Greenleaf & Cottier, 2018; OVIC, 2018). Some of these limitations that require critical review are as summarized in Table 1.

Even where there are principles in place within the policy framework – such as consent – which in the ECOWAS Act is stipulated thus:

[4]https://gdpr-info.eu/

[5]Organisation for Economic Co-operation and Development

[6]OECD Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013). Accessed April 5, 2019: http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Consent of the data subject is any manifestation of specific, unequivocal, free, informed and express will by which the data subject or his legal, judicial or agreed representative accepts that his personal data be processed either manually or electronically

How can consent be '*specific, unequivocal and informed*' if a data controller does not have full knowledge of the ultimate data processing purpose as is rife with artificial intelligence systems?

These policy limitations are critical for review in the era of artificial intelligence deployments as algorithmic analytics feed on large datasets from connected devices which may not necessarily be collected via a conscious and transparent mechanism; as well as the unintended consequences of data processing especially personal data. As opined by Cate and Dockery (2019), in rethinking AI-related data protection and privacy policy frameworks, critical appraisal should be given to a shift towards a risk-biased use-based approach of data stewardship from data subjects to data controllers especially with respect to issues such as consent. This will help repurposing the objective of data protection and privacy from terms of collection to risks and impacts of processing and usage in-contexts, in order to achieve more optimal balance between valuable data flows and data protection and privacy.

Table 1: ECOWAS 2010 data protection Act in comparison to other regional policy frameworks (Adapted from Pätsch, 2018)

Principles	ECOWAS (2010)	OECD (2013)	GDPR (2016)
Automated decision making: Prohibition	Yes	No	Yes
Automated decision making: Right to object	No	No	Yes
Automated decision-making: Right to logic information	No	No	Yes
Data controller obligation: Data protection by default	No	No	Yes
Data controller obligation: Data protection by design	No	No	Yes
Data controller obligation: Notification	No	Yes	Yes
Data controller obligation: Risk or impact assessments	No	Yes	Yes
Data subject right: Data portability	No	No	Yes
Data subject right: Right to be forgotten	No	No	Yes
Liability: Data controller and processers	No	No	Yes
Territorial scope: Data has to be processed according to rules of the data subject jurisdiction no matter where the processing is taking place	No	No	Yes
Trans-border data flow: Privacy may not restrict free flow of personal data	No	Yes	Yes

3. Conceptual framework

In the context of this research therefore and to answer the research questions prior stated, an ontological model framework as put forward by Greiman (2018) will be adopted (Figure 1). The model operates as a mechanism of interrogating a shared understanding of a unifying structure, explicating the challenges and misunderstandings of a cyber policy governance framework. According to the *European Agency for Network and Information Security* (ENISA), an ontological model incorporates the conceptualization of the attributes and processes between interrelating entities in a multilateral policy framework.

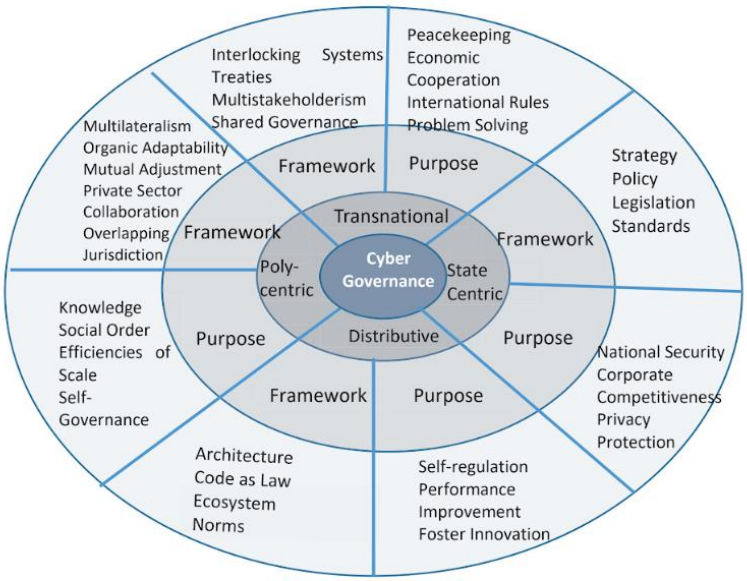

Figure 1: Ontological model for cyber governance (Greiman, 2018)

The model will be applied to within the transnational lens to interrogate cyber policy harmonization challenges especially with regards to artificial intelligence in Africa, and will provide the conceptual basis for the research design and implementation. The ontological development with regards to this methodology entails:

- Evaluation of AI-related data protection and privacy governance frameworks in the comprising transnational entities, identifying the key stakeholdership and actors in each domain
- Determining the commonalities and differences among the interrelating transnational entities and critical areas for collaboration and coordination with respect to AI-related data protection and privacy (both horizontally and vertically)
- Evaluating the challenges, social benefits, spillover effects and costs of a harmonized data protection cyber policy between the transnational entities in order to proffer alternative stabilization arrangements

4. Research Approach

Relying on the ontological model, the research design for the study will comprise a comprehensive review and analysis of pertinent cyber governance literature, with a focus on data protection cyber policy in relation to artificial intelligence. The objective will be to highlight the critical gaps, explore the challenges and opportunities, and generate new thinking on regional and continental-level cyber governance mechanisms on the continent. The output of the literature analysis will be fed onto semi-structured interviews with cyber governance professionals and policy experts on the continent at both the governmental and inter-governmental levels in relation to the research questions prior highlighted (see Trauner, 2011). Sampling will be based on a purposive strategy in order elucidate the varying perspectives that are based on the experiences of the respondents in the traditions of Maurer (2011) and Solum (2009). A sampling scope consisting of about 15 to 20 respondents is proposed including relevant representatives of the African Union and ECOWAS, civil society, as well as regional cyber policy experts on the continent.

To ensure consistency and enhance the reliability of findings, an interview protocol will be developed and structured to ensure that the research objectives are comprehensively covered. Transcribed records of interview sessions will then be incorporated with session notes and analyzed using a constant comparison technique to code the emergent themes in relation to AI-related transnational cyber policy harmonization on the continent. The constant comparison technique is a qualitative analytical method that compares relatable data as they are applicable to the different emerging categories of theoretical analysis. In this regard, the generation of hypothesis is progressive as it emerges from the data coding and analysis. The output from this process will be triangulated with content analysis of cyber policy reports that will be validated both internally and externally in order to reduce confirmation bias using source criticism (see Kipping et al., 2014). In this sense, triangulation is the synthesis of a minimum of two data sources or analytic processes within the same study in order to enhance the reliability of findings by cross-validating similarities; in this case - interviews analysis and content analysis of policy reports. Source criticism on the other hand is simply validating the currency and authorship credibility of a document (internal) as well as the evidential value it provides in relation to other data sources (external). The commonalities and differences among the interrelating transnational entities with respect to varying structural arrangements for AI-related cyber governance will be analyzed using the disciplined-configurative comparative approach for qualitative social science studies (see Kaarbo & Beasley, 1999; Thomas, 2011). This is an interpretive method that compares very small-N cases using general variables for purposes of description and explanation in order to provide a common focus. The general variables are defined on the basis of the theoretical hypothesis generated after qualitative analysis.

5. Expected conclusions (research outputs) and policy recommendations

The study seeks to contribute to the research on transnational cyber governance, with focus on AI-related policy mechanisms at the regional and continental levels in Africa, using the ontological model framework. This will highlight the institutional challenges of transnational AI regulation on the continent whether ex post or ex ante as well as provide a pathway for effective data protection policy making in this regard. In contributing to knowledge, the study seeks to bridge the scholarship gap on transnational AI cyber regulation specifically through the lens of institutional configuration.

In the policy practitioner domain, outcomes from the research will lend an evidence base to adapting alternative transnational cyber policy coordination on the continent with regards to enhancing outcomes for AI-related cyber security, data protection and privacy. The comparative analysis among the transnational entities with respect to varying structural arrangements for AI-related cyber governance will elucidate specific attributions and their unique contributions in the development of a coherent transnational cyber governance framework (see Schneider & Hyner, 2006; Kölliker, 2006). In summary, the research outputs expected from the study will include:

- Alternative transnational approaches to data protection cyber policy and regulation especially in relation to peculiarities of artificial intelligence in the African context
- Novel perspectives on regional and continental-level data protection policy harmonization mechanisms in relation to artificial intelligence on the continent
- Assay on the commonalities and differences among the interrelating transnational entities with respect to varying structural arrangements for AI-related data protection and privacy
- Provide significant pathway for cohesive AI-related data protection cyber governance at the regional-level

References

Bostrom, N., Dafoe, A., & Flynn, C. (2018). Public Policy and Superintelligent AI: A Vector Field Approach. Governance of AI Program, Future of Humanity Institute, University of Oxford: Oxford, UK. Accessed January 24, 2019: https://pdfs.semanticscholar.org/9601/74bf6c840bc036ca7c621e9cda20634a51ff.pdf

Brattberg, E. & Rhinard, M. (2012). The EU as a Global Counter-Terrorism Actor in the Making. European Security, Vol. 21, No. 4, pp. 557–77

Burke-White, W. W. (2003). Regionalization of International Criminal Law Enforcement: A Preliminary Exploration. Tex. Int'l LJ, 38, 729.

Campolo, A., Sanfilippo, M., Whittaker, M.,& Crawford, K. (2017). AI Now Report. Accessed March 27, 2019: https://ainowinstitute.org/AI_Now_2017_Report.pdf, p 3

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor?. JCMS: Journal of Common Market Studies, 55(6), 1254-1272. Accessed January 22, 2019:https://onlinelibrary.wiley.com/doi/full/10.1111/jcms.12575

Cate, F.H.& Dockery, R. (2019). Artificial Intelligence and Data Protection: Observations on a Growing Conflict. Accessed April 5, 2019: https://ostromworkshop.indiana.edu/pdf/seriespapers/2019spr-colloq/cate-paper.pdf

Dafoe, A. (2018). AI Governance: A Research Agenda. Governance of AI Program, Future of Humanity Institute, University of Oxford: Oxford, UK. Accessed January 24, 2019: https://www.fhi.ox.ac.uk/wp-content/uploads/GovAIAgenda.pdf

Evanoff, K.& Roberts, M. (2017). A Sputnik moment for artificial intelligence geopolitics. Council on Foreign Relations, blogpost, Accessed January 21, 2019: https://www.cfr.org/blog/sputnik-moment-artificial-intelligence-geopolitics

Gadzala, A. (2018). Coming to Life: Artificial Intelligence in Africa Issue Brief November 2018. Accessed January 22, 2019:https://www.atlanticcouncil.org/images/publications/Coming-to-Life-Artificial-Intelligence-in-Africa.pdf

Greenleaf, G., & Cottier, B. (2018). Data Privacy Laws and Bills: Growth in Africa, GDPR Influence. Accessed April 2, 2019: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3212713

Greiman, V. (2018). Reflecting on Cyber Governance for a new World Order: An Ontological Approach. In ECRM 2018, 17th European Conference on Research Methods in Business and Management (p. 148). Academic Conferences and publishing limited. Accessed January 22, 2019:https://books.google.com.ng/books?hl=en&lr=&id=gU9mDwAAQBAJ&oi=fnd&pg=PA148&dq=models+Artificial+intelligence+cyber+policy+harmonization+internet+governance+Africa&ots=Etf6aYoZUY&sig=-aXKfuk7fs7p8wP6W7cn3P_x5jI&redir_esc=y#v=onepage&q&f=false

Kaarbo, J., & Beasley, R. K. (1999). A practical guide to the comparative case study method in political psychology. Political Psychology, 20(2), 369-391.

Kipping, M., Wadhwani, R. D., &Bucheli, M. (2014). Analyzing and interpreting historical sources: A basic methodology. In M. Bucheli& R. D. Wadhwani (Eds.), Organizations in time: History, theory, methods (pp. 305–325). Oxford, England: Oxford University Press.

Kölliker, A. (2006). Conclusion I: Governance Arrangements and Public Goods Theory: Explaining Aspects of Publicness, Inclusiveness and Delegation. In New Modes of Governance in the Global System (pp. 201-235). Palgrave Macmillan, London.

Kuner, C., Cate, F. H., Lynskey, O., Millard, C., Ni Loideain, N., &Svantesson, D. J. B. (2018). Expanding the artificial intelligence-data protection debate. Accessed March 27, 2019: https://academic.oup.com/idpl/article/8/4/289/5299551

Lehmkuhl, D. (2006). Resolving Transnational Disputes: Commercial Arbitration and Linkages Between Multiple Providers of Governance Services. In New Modes of Governance in the Global System, pp. 101-124. London: Palgrave Macmillan.

Makulilo, A. B. (2015). Myth and reality of harmonisation of data privacy policies in Africa. Computer Law & Security Review, 31(1), 78-89.

Mattoo, A., & Meltzer, J. P. (2018). International data flows and privacy: The conflict and its resolution. Journal of International Economic Law, 21(4), 769-789.

Maurer, T. (2011). Cyber norm emergence at the United Nations. Science, Technology, and Public Policy Program. Accessed January 22, 2019:https://www.belfercenter.org/sites/default/files/files/publication/maurer-cyber-norm-dp-2011-11-final.pdf

Mussington, D., Arnold, B. J., Dupont, B., Hilts, S., Grayson, T., Leuprecht, C., ... &Tupler, J. (2018). Governing Cyber Security in Canada, Australia and the United States. Accessed January 22, 2019:https://www.cigionline.org/sites/default/files/documents/SERENE-RISCweb.pdf

Office of the Victorian Information Commissioner (OVIC, 2018). Artificial intelligence and privacy. Issues paper. Accessed March 27, 2019: https://ovic.vic.gov.au/wp-content/uploads/2018/08/AI-Issues-Paper-V1.1.pdf

Pätsch, S. (2018). How Brussels is emerging as a global regulatory superpower, establishing its data protection standard worldwide. Masters Thesis, Lund University Sweden. Accessed April 5, 2019: http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8940309&fileOId=8940310

Schneider, V., &Hyner, D. (2006). Security in Cyberspace: Governance by Transnational Policy Networks. In New Modes of Governance in the Global System (pp. 154-176). Palgrave Macmillan, London.

Sofaer, A. D., & Goodman, S. E. (2001). Cyber crime and security. The transnational dimension. The transnational dimension of cyber crime and terrorism, 1-34.

Solum, L. B. (2009). Models of internet governance. Internet governance: infrastructure and institutions, 48-91.

Thomas, G. (2011). A typology for the case study in social science following a review of definition, discourse, and structure. Qualitative inquiry, 17(6), 511-521.

Trauner, F. (2011). The internal-external security nexus: more coherence under Lisbon?. Accessed January 22, 2019:https://www.ies.be/files/op89_The_internal-external_security_nexus.pdf

Turianskyi, Y. (2018). Balancing Cyber Security and Internet Freedom in Africa. Accessed January 21, 2019: https://www.africaportal.org/publications/balancing-cyber-security-and-internet-freedom-africa/