African Journal on Privacy & Data Protection

Editorial ~ Volume 1, 2024

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Dr Akinola Akintayo
Managing Editor
March 2024