

Digital Colonialism Beyond Surveillance Capitalism? Coloniality of Knowledge in Nigeria's Emerging Privacy Rights Legislation and Border Surveillance Practices

Social & Legal Studies

1–22

© The Author(s) 2024



Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/09646639241287022

journals.sagepub.com/home/sls**Samuel Singler** *University of Essex, UK***Olumide Babalola***University of Portsmouth, UK*

Abstract

This article examines the impact of privacy rights norms and North–South technological diffusion on the development of Nigeria's emerging legal regime for data governance, and the relationship between this legal regime and the digitalisation of border control in Nigeria. We show that federal data protection regulations and border control technologies in Nigeria are not characterised by the extractive logics of surveillance capitalism, which is the focus of several contemporary critiques of 'digital colonialism'. Nonetheless, the country's data governance regime and its digital borders have been shaped by Northern-produced norms, practices, and technical tools – interacting with the interests and agency of local actors – through both legislative and technological influences. Critically analysing the co-production of law and digital infrastructures highlights the coloniality of knowledge relating to data protection, privacy rights, and digital mobility control. These cases suggest that digital colonialism can be productively analysed beyond the scope of surveillance capitalism.

Corresponding author:

Samuel Singler, Department of Sociology and Criminology, University of Essex, Colchester, UK.

Email: samuel.singler@essex.ac.uk

Keywords

borders, data protection, digitalisation, infrastructures, mobility, Nigeria, postcolonialism, surveillance

Introduction

Nigeria is undergoing a rapid societal ‘digital transformation’ supported by a range of private and public external actors, including transnational telecom companies, international organisations such as the International Telecommunication Union, and Global North states (Pharaon, 2023). The European Union (EU), for instance, pledged 160€ million in grants and a further 660€ million in loans as part of the EU–Nigeria digital economy package from 2021 to 2024 (European Union, 2022). Against this backdrop of digitalisation, policymakers in the country issued the Nigeria Data Protection Regulation (NDPR) in 2019 followed by the Nigeria Data Protection Act (NDPA) of 2023. While formally based on Section 37 of the 1999 Nigerian Constitution, which outlines a constitutional right to privacy, the NDPR consciously mirrored the EU’s General Data Protection Regulation (GDPR) and demonstrated the influence of Northern-produced privacy rights norms.

During the drafting of the new data protection legislation, external actors such as the International Organization for Migration (IOM) supported the digitalisation of Nigeria’s external borders. This digitalisation of mobility control was enacted through the deployment of a new digital border control technology, the Migration Information and Data Analysis System (MIDAS) (Singler, 2021). Concerned that new privacy legislation might in the future limit the collection or retention of sensitive personal data at the border, IOM officials were involved in consultations with Nigerian federal officials to ensure the inclusion of national security- and crime control-related exceptions in the final version of the NDPA. These officials actively sought to ensure that biometric surveillance at the border would be protected against privacy-focused limitations in the final legislation. Their arguments were informed by conceptions of digital border control necessarily including expansive data collection and data sharing between immigration and law enforcement authorities. Paradoxically, these arguments were rooted in the discourse of human rights, which was employed not to curtail expansive surveillance at the border but rather to demonstrate the rights-based ‘expertise’ of the Northern-funded IOM, legitimising its interventions in Nigeria’s emerging digital border surveillance regime (Sokhi-Bulley, 2019).

Several disciplines – including law, socio-legal studies, criminology, and privacy studies – are undergoing necessary and complex processes of decolonisation and Southernisation (Aliverti et al., 2021; Arora, 2019). Researchers working within and across these disciplines have highlighted the long-standing dominance of Northern epistemological assumptions and empirical contexts even in critical scholarship (An-Naim, 2021). Correcting the epistemological and empirical underrepresentation of the Global South has now rightly been recognised as not only a normatively desirable endeavor but also an analytically invaluable opportunity for ‘methodological and theoretical innovation’ (Aliverti et al., 2021: 304). In this article, we contribute to the

ongoing decolonisation and Southernisation projects by critically analysing new data protection legislation in Nigeria, also examining how these new laws have shaped – and have been shaped by – the development of new digital border control tools in recent years.

By examining the NDPA and MIDAS in Nigeria, we argue that the enactment of a ‘universal’ right to privacy in Nigerian legislation and at the country’s new digital borders is underpinned by Northern-produced legal norms, practices, and technologies, yet translated into the Nigerian context according to the cultural histories, interests, and agency of local actors themselves. We demonstrate how legal and practical frameworks for privacy and mobility control have been reshaped by the colonial encounter and postcolonial epistemic influences since independence. The postcolonial dimensions of privacy legislation and digital border surveillance in Nigeria reflect the enduring coloniality of knowledge in terms of how ‘universal’ rights shape both the law on the books and the law in action (Feenan, 2013; Quijano, 2007).

Decolonial engagement with global data privacy regulations and their practical enactment requires an understanding of how Northern-produced ‘best practices’ and standards, such as the EU GDPR, are promoted globally by diverse state and non-state actors, and how the supposedly ‘universal’ rights that these standards seek to secure are translated into local practices in the Global South (Arora, 2019: 369). We situate the development of data protection legislation and digital border control systems within the broader ‘datafication’ of global mobility control (Frowd, 2024) and demonstrate that Nigeria’s emerging regime for data governance has been co-produced by the interaction of legal and technological influences. We draw on the ‘infra-legalities’ approach (Sullivan, 2022: S33, original emphasis), which ‘requires studying law or regulation and data infrastructures *together* as co-emergent’. This approach examines how lawmaking and regulatory techniques influence the deployment of new digital technologies, while also looking ‘*below* the law towards mundane socio-technical practices in global security governance’ (Sullivan, 2022: S33, original emphasis). Below, we outline how legal norms codified in Global North frameworks such as the GDPR have shaped the law ‘from above’, while the IOM-led digitalisation of Nigeria’s borders has shaped Nigeria’s new data protection regulation ‘from below’.

In the next section, we outline a critical perspective on analysing the co-production of law and technology, with a particular focus on how this approach can help deconstruct the coloniality of both legal and technical knowledge in postcolonial contexts. We then explain our methodological approach, combining qualitative legal analysis with elite interviews and field observations in Nigeria. The section ‘Coloniality of Legal Knowledge in Nigeria’s Emerging Regime for Data Governance’ analyses the the legal norms that shaped the NDPA ‘from above’, and the section ‘Coloniality of Sociotechnical Knowledge at Nigeria’s Digital Borders’ examines how Northern-backed sociotechnical expertise influenced the digitalisation of Nigeria’s external borders, which shaped the data protection legislation ‘from below’. Ultimately, we demonstrate that Nigeria’s emerging legal regime for privacy and data protection is co-produced by both legal and socio-material processes, both of which involve the interplay between postcolonial epistemic hierarchies and local agency.

The Co-production of Law and Technology in Postcolonial Contexts

Analysing contemporary developments in national data protection legislation and the enactment of these regulations in the Global South requires unpacking the historical relationship between Northern-produced legal norms and colonial exploitation and hierarchy (Zumbansen, 2019). In postcolonial contexts such as Nigeria, the modern state structure, including its territorial limits and legislative frameworks, was largely inherited from British colonial rule (Saleh-Hanna, 2008). In such contexts, it is important to highlight how Northern ‘legal technologies’ have historically contributed to the suppression, exploitation, and removal of local populations ‘through legal regimes that did not recognize their histories, territories, or forms of legal authority’ (Mawani, 2021: 50).

Such insights are not merely of historical interest. They are also relevant to contemporary analyses of legal and sociotechnical practices from a decolonial and Southern perspective. The notion of ‘universal’ human rights — including privacy as enshrined in international legal frameworks such as Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) — has important parallels to earlier civilisational discourses. As Abdullahi Ahmed An-Naim (2021: 1–2) has argued, the formerly colonial Global North states set the agenda and determine dominant understandings of rights, and then police the enactment of these ‘universal’ rights across the globe:

The power of developed states to influence the human rights policies and legislation of developing states always flows from former colonial and richer countries of the Global North against former colonies and poorer countries of the Global South, and never the other way around. [...] Such dependency is legitimized by affiliation to human rights, thereby hiding the underlying historical hegemony and exploitation.

The crucial task is to examine how supposedly ‘universal’ rights such as the right to privacy are promoted globally by Northern states and Northern-backed actors such as large international organisations, and how these Northern-produced discourses interact with local understandings and agency to produce novel constellations of legal and political practices surrounding individual rights. Accounting for differences in understandings of privacy rights, as well as who should be responsible for upholding these rights, is important due to how digital surveillance technologies are already implicated in various forms of social discrimination (Ugwudike, 2020).

A key focus of ongoing human rights debates is the right to privacy in the context of data protection and digital surveillance (Arora, 2019). Several authors have analysed the contemporary digitalisation of society and politics across the African continent and other postcolonial contexts in terms of ‘digital colonialism’ (Kwet, 2019). Digital colonialism is a useful framework for highlighting how digitalisation in Global South contexts is often driven by the profit motives of transnational corporations engaged in economic extraction and dispossession, (post)imperial control of technological infrastructures, and public–

private forms of North–South control and influence (Coleman, 2019). In this view, digitalisation in the Global South is underpinned by the global expansion of ‘surveillance capitalism’, which foregrounds ‘the collection, extraction, and analysis of users’ data to perform behaviour prediction and modification used for economic profit’ (Firmino et al., 2019: 207; Zuboff, 2019).

However, federal data protection legislation and border control lie outside of the surveillance capitalist focus on economic extraction and imperial dispossession by private corporations. Although surveillance capitalist practices are structured by a background of state regulation, federal legislation in Nigeria is not directly shaped or sponsored by private corporations beyond the fact that the federal government has an economic interest in continued e-commerce and trade with Global North countries (Makulilo, 2013). Economic arguments were not very effective in generating political support for federal data protection legislation over the past two decades (Iwobi, 2017: 37–38). Moreover, data protection regulations are often used, at least in principle, to ‘limit the power of surveillance capitalism’ relative to the authority of public institutions (Aho and Duffield, 2020: 187). At its borders, Nigeria has opted to deploy MIDAS as opposed to alternatives sold by private companies precisely to retain sovereign control of the digital data collected from border crossers and avoid dependence on private companies. While surveillance capitalism no doubt underpins broader digitalisation processes in Nigeria (see, e.g. Oyedemi, 2020), this framework is less helpful for understanding Nigeria’s emerging regime for data protection and border control. The influence of private corporations is at best highly indirect in these contexts, and emerging legislation is likely to curtail rather than intensify extractive surveillance capitalist practices (Choroszewicz and Mäihäniemi, 2020).

Nonetheless, we argue that ‘digital colonialism’ can be understood in broader terms than just economic extraction, following Barbara Arneil’s (2024: 3) analysis of colonialism as an ideology ‘animated by an internalized, penetrative, and productive form of power that seeks to segregate and “improve” “backward” people(s) from within and “improve” “waste” lands’. This perspective on colonialism also maps onto important discussions of the colonality of knowledge and the colonality of power (Quijano, 2000). These notions expand critical postcolonial analyses beyond a focus on the extractive mechanisms of transnational capital accumulation to include a focus on the epistemic dimensions of global hierarchy, rooted in colonial conceptions of the universality and rationality of Northern-produced knowledge to the detriment and exclusion of Southern alternatives (Quijano, 2007). Such epistemic hierarchies underpin contemporary forms of knowledge production about global ‘best practices’ in fields such as data governance and mobility control. In these contexts, coloniality endures ‘in the essentialized difference between periphery and metropole, which constructs the former as an anomalous site in need of intervention along universalized global blueprints’ (Jegen, 2023: 3).

Technology-related legislative norms on privacy rights and data protection are developed against the background of postcolonial hierarchies. These norms are subsequently translated into local practices by Southern actors. A socio-legal approach is helpful in examining what happens to the discourse of a ‘universal’ right to privacy when we observe practices of lawmaking and ‘law on the books’, as well as when we examine

the 'law in action' (Feenan, 2013: 5). A specifically postcolonial perspective on socio-legal studies requires uncovering the 'underlying, deeper as well as systematic conditions out of which legal challenges emerge locally' (Zumbansen, 2019: 915). Rather than assuming that legal frameworks are first established and only have societal effects once 'in action', or conversely that law is merely responsive to sociopolitical (or technological) changes, instead this perspective views law and society as 'co-emergent' or 'co-produced' (Lee et al., 2018).

While the insights of critical socio-legal studies can be applied to several fields of law and society, the idiom of 'co-production' is particularly pertinent for understanding the relationship between legal frameworks governing new digital technologies on one hand, and ongoing material practices of digitalisation and the development of technological infrastructures on the other hand. The notion of 'co-production' was influentially deployed by Sheila Jasanoff (2004) in the field of science and technology studies (STS) to describe the dynamics of how technological developments and sociopolitical practices not only influence one another but are literally co-constituted. In this view, technical knowledge and social order are co-produced in the sense that 'ordering knowledge impacts the ordering of society, and therefore understanding how the making of knowledge is organized, who participates, and who has rights and responsibilities to speak authoritatively about knowledge is crucial for understanding how solutions come to being' (Martins and Jumbert, 2022: 1443).

Gavin Sullivan (2022: S35, original emphasis) has drawn on the idiom of co-production to argue that new security and surveillance technologies and the regulatory frameworks that govern them 'are not defined in isolation from each other, but *in and through* their relational networks'. Sullivan (2022)'s 'infra-legalities' approach sits within the broader ongoing effort to more critically analyse the socio-material nature of legal infrastructures. According to this perspective, a critical analysis of emerging regimes for data governance requires analysing both the 'interconnected legal norms, practices, and institutions' that shape these regimes from above, as well as the material objects and technologies that influence them from below and through which legal frameworks are enacted (Byrne et al., 2023: 10).

Analysing the development of privacy rights and digital borders in Nigeria simultaneously allows us to examine the co-constitutive relationship between law, society, and technology. We describe the influence of Global North norms relating to data protection and privacy rights on Nigeria's emerging legislative frameworks as shaping the field of digital society in a 'top-down' manner insofar as legislation represents the formalised expression of state authority. In turn, technical developments and standards that are developed and adopted at Nigeria's digital borders, and which subsequently shape the discourse and legislation surrounding privacy rights, can be viewed as an expression of the co-production of law and technology in a 'bottom-up' fashion. Importantly, given the existing postcolonial epistemic and socioeconomic hierarchy, *both* top-down legislative and bottom-up technological dynamics of the politics of privacy rights in Nigeria are shaped by Northern norms, standards, discourses, and varying extents of direct and indirect political influence by external actors in interaction with the agency of Nigerian authorities.

Methods and Data Collection

The empirical analysis presented below is based on data collected through legislative analysis – and personal involvement in privacy litigation in Nigeria – by one author, and qualitative fieldwork focusing on the IOM’s border-related interventions in Nigeria by the other author. The legislative analysis focused on relevant secondary legal scholarship as well as official legal documentation produced by Nigerian federal authorities that related directly to the NDPR and NDPA. The analysis was based on a qualitative approach to non-doctrinal legislative analysis, which focuses on the ‘social factors involved and/or the social impact of current law and practice’ (Dobinson and Johns, 2017: 23). Analysing how the NDPR eventually evolved into the NDPA demonstrates the influence of Global North norms in shaping the final Act; in turn, the codification of these norms in the NDPA is likely to serve as a critical juncture heavily shaping the future of Nigeria’s legal regime for data governance (Linos and Carlson, 2017).

The fieldwork was conducted during three months in the summer of 2021, as part of a broader research project examining the impact of MIDAS on the global merger of border control and criminal justice (see Singler, 2024). Fieldwork observations in Abuja, Nigeria, were complemented by elite interviews conducted both online and in person between January–September 2021. Interview participants included senior IOM officials and Nigerian federal officials, who are categorised as elites due to their ‘important social networks, social capital and strategic positions’ in the field of Nigerian data protection legislation and border control practices (Harvey, 2011: 433). The empirical data presented below also includes field notes taken during data protection-related workshops and meetings with IOM and Nigerian federal officials in Abuja. All interviews were manually transcribed by the researcher and interview transcripts as well as fieldnotes were analysed and thematically coded using NVivo (Hilal and Alabri, 2013). During interviews and field observations in Nigeria, the themes of ‘modernisation’ and ‘human rights expertise’ emerged as key dimensions for understanding how IOM officials have sought to influence Nigeria’s emerging data protection and privacy rights regimes.

Coloniality of Legal Knowledge in Nigeria’s Emerging Regime for Data Governance

The Development of Privacy Legislation in Nigeria

The trajectory of Nigeria’s legal evolution of the right to privacy is deep-rooted in the country’s constitutional conversations around the bills of rights. Privacy first appeared in 1954 under the Lyttleton Constitution even though the provisions on fundamental rights were ‘relegated’ to the sixth schedule of the Constitution (*J. S. Olawoyin v. Attorney-General, Northern Region, Nigeria*, 1960). Since its constitutional debut in 1954, the right to privacy has appeared in successive constitutions under varying nomenclature, either as the ‘right to private life’ or ‘right to private and family life’ (Thym, 2008).

The right to privacy together with the entire bill of rights was inspired and influenced by the European Convention on Human Rights (ECHR). The significant role played by the ECHR on Nigeria's constitutional right to privacy (along with the bill of rights) was judicially narrated by Justice Adolphus Karibi-Whyte in 1980: '[The 1957 Constitutional Conference] followed closely the terms of the European Convention on Human Rights, adopted by the United Kingdom parliament barely eight years previously' (*Shugaba Abdulrahman Darman v. The Federal Minister of Internal Affairs and Others*, Nigeria, 1980).

Considering the 'law in action', privacy rights were under-litigated and under-researched for decades despite judicial declarations of their pre-eminence in the 'committee' of fundamental rights (Kalu and Ewuzie, 2021). After about six decades of successive constitutional provision on the right to privacy in Nigeria, data protection surfaced, first under various sectoral legislation and then in the mold of a dedicated but subsidiary legislation – the NDPR of 2019 – effectively setting up a legal framework for data protection in the country (Babalola, 2022). Prior to the issuance of the NDPR, the Nigerian parliament unsuccessfully attempted to legislate data protection until the eventual passage of the renamed NDPA 2023 into law on 12 June 2023. The law effectively established a data protection authority to exclusively regulate data protection affairs in Nigeria, sparking a new chapter in the country's legal framework for data protection.

Translating 'Universal' Privacy Rights to Postcolonial Contexts

The inspiration received by the Nigerian constitutional draftsmen from the ECHR is evident in the convention's guarantee of 'private and family life' being mirrored in Nigeria's provision of the 'right to private and family life' in a marginal note to the constitutional right to privacy. Several authors refer to 'private and family life' while discussing the right to privacy under Nigerian law, even though the body of Section 37 of the Nigerian Constitution omits the protection of family life (Abdulrauf and Daibu, 2016). While the marginal note under the Nigerian Constitution recognises 'private and family life' as provided under Article 8 of the ECHR, the textual provisions and consequent court decisions do not show maximum appreciation of latitude offered by the larger concept of family life.

The Nigerian Supreme Court demonstrated the more constrained view on privacy excluding family life in the decision in *Uchechi Nwachukwu v. Henry Nwachukwu & Anor* (2018). In that instance, a woman sued her husband for exposing her HIV status and engaging thugs to throw her things out of the matrimonial home. The Supreme Court viewed this case as a matrimonial dispute rather than a matter relating to the right to 'private and family life'. From the perspective of an ECHR-based understanding of private and family life, a broader concept that embodies an individual's 'relationship with other persons and the outside world', the court rejected expanding the extent of rights-based protections (Kilkelly, 2003). The decision reflected the continued disjuncture between local privacy beliefs and international privacy rights regarding personal boundaries in a family context, on the one hand, and the limited support for privacy legislation as a preferred enforcement mechanism of individual rights in Nigeria, on the other hand.

Historically, the National Human Rights Commission (NHRC) was established in Nigeria to ‘deal with matters pertaining to human rights, monitor and investigate human rights violations and assist victims’ (Tabiu, 2001: 553). However, the limited institutional value placed on privacy has diverted the NHRC’s attention away from privacy rights. There exists no verifiable or publicised report on the Commission’s activities or strategies for the enforcement or development of the right to privacy or data protection in Nigeria, as most appraisals have focused on other more ‘valuable’ rights (Nnamani, 2011). Since independence, no Nigerian public agency was assigned the function of regulating privacy or data protection until the National Information Technology Development Agency (NITDA) positioned itself as a self-appointed data protection authority through its issuance of the NDPR. Even though the NDPR recognises other ‘relevant authorities’ eligible to regulate data protection, NITDA performed the role until its replacement by the Nigeria Data Protection Bureau (NDPB) in February 2022.

Nigeria’s emerging legal regime for data governance has become a key site at which the disjuncture between local privacy beliefs and international privacy rights is currently being narrowed. Nigeria substantially owes its initial regulation of data protection to the EU GDPR. This influence was confirmed by NITDA: ‘The NDPR as a subsidiary legislation was innovatively crafted to match all the foundational principles of data protection from Convention 108+, Malabo Convention on Cybersecurity and Data Protection to the General Data Protection Regulation (GDPR)’ (NITDA, 2020: 3). The NDPR was enacted under the 2007 NITDA Act, demonstrating that IT development constituted a primary impetus for the development of national data protection regulation alongside international privacy rights standards (KPMG, 2019). As we outline in more detail below, digital infrastructures and privacy law are, in this way, continually being co-produced and shaped by Global North influences across both technical and legal contexts.

In addition to the regulator’s documented admission, Nigerian academics have also written at varying times on the GDPR’s status as a standard for the NDPR (Akintola and Akinpelu, 2021). Reviews of the Nigerian data protection framework have also frequently used the GDPR as a yardstick, pointing out that the NDPR mirrored the GDPR in crucial respects (Babalola, 2021). With respect to the cross-border transfer of personal data, the NDPR copied the GDPR model in relation to adequacy requirements with slight adjustments to the entity empowered to make adequacy decisions. The newly enacted NDPA, however, duplicates the European provision but with several exceptions, which seem to allow for the unlimited cross-border flow of personal data.

While the NDPA undeniably draws inspiration from the European model in its provisions on principles of data processing and rights of data subjects, differences remain in its omission of sexual orientation from the definition of sensitive data; categorising data controllers along the line of their ‘importance’ to the economy; and fixing the age of consent at 18 years and recognising a standalone right to withdraw consent. Nigeria’s anti-same-sex legislative stance appears a justification for its replacement of ‘sexual orientation’ as sensitive data with ‘sexual life’. The requirement to register with the Information Commissioner’s Office by paying a data protection fee in the United Kingdom influenced the inclusion, in the Nigerian Act, of a requirement that data controllers of major importance be registered with the Nigeria Data Protection Commission. The Nigerian provision on automated decision-making (ADM) is a substantial replication of

the GDPR's provision even though the dynamics are different across these contexts. While ADM and profiling are a regular feature in the European business sector especially in banking, mortgages, crime detection, insurance, and e-commerce, such examples are not easily found in the Nigerian ecosystem. Significantly, regulatory limits to ADM have been used to curtail excessive and invasive surveillance capitalist practices in EU countries, which again points to the limits of analysing Nigeria's emerging regime for data governance solely through the lens of private economic extraction (Choroszewicz and Mäihäniemi, 2020).

These similarities and differences are telling in terms of the coloniality of legal knowledge despite the lack of directly identifiable surveillance capitalist dynamics. The influence of Northern-produced rights-based discourses and frameworks is clear in Nigerian legislation. For instance, the anticipation of ADM and digital profiling reflects a teleological view of technological modernisation. Yet, local beliefs, practices, and political interests periodically intervene to produce novel constellations of privacy rights legislation and enforcement in the country. The Nigerian approach to 'sexual orientation' and other LGBTQ-related data also demonstrate how contemporary legislation maps onto colonial histories of lawmaking and changing notions of 'civilisation' and 'universal' rights. The origins of Nigerian anti-LGBTQ laws lie in the British colonial-era Penal Code and Criminal Code (Chimakonam and Agada, 2020). These colonial laws were based on both Christian puritanical ideas of 'civilized' behaviour and an 'orientalized' view of the colonies as potential sites of sexual promiscuity. The legislation has endured in the postcolonial era and is now also underpinned by contemporary widespread support among the Nigerian public for the continued criminalisation of homosexuality on religious grounds (Chimakonam and Agada, 2020).

Due to changing normative ideas in the Global North, however, despite the colonial origins of anti-LGBTQ laws in Nigeria and elsewhere, such legislation is now viewed by Global North states, international institutions, and civil society actors as an affront to universal rights and moral 'progress' (Kollman and Waites, 2009). Nigeria, among other postcolonial states, is condemned by global human rights 'experts' and NGOs for continuing to enforce what was a 'colonial imposition' but which is now framed 'as something that is essentially African' (Ibrahim, 2015: 265). To be very clear, rectifying the violation of LGBTQ rights constitutes a pressing and important political issue globally. Nonetheless, this example demonstrates how earlier colonial legal impositions can become normatively reframed in the postcolonial era, and how this reframing can then be used by Global North actors to reshape legislation in the Global South in the name of 'universal' human rights. So too, differences between Global North and Nigerian conceptions of privacy have recently been recast as a lack of formalised privacy legislation, which the more Global North-inspired NDPA is meant to address.

The foregoing discussion demonstrates how international obligations and standards have inspired recent privacy legislation in Nigeria, and how the coloniality of legal knowledge is reflected both in the colonial legacies of rights-based legislation in the country as well as contemporary inequalities in epistemic power to redefine human rights norms and best practices globally. Importantly, in the context of state-backed privacy legislation, these Northern influences are not directly connected to the contemporary logics of 'surveillance capitalism', which would suggest that transnational

private companies are the key actors seeking to expand opportunities for economic extraction and dispossession through the collection of digital data (Coleman, 2019). Yet, examining the coloniality of legal knowledge highlights the enduring epistemic hierarchies that underpin differential power to determine how ‘universal’ privacy rights should be codified (An-Naim, 2021).

Domestic Agency and in the NDPA ‘In Action’

Nigerian state authorities are by no means simply forced to adopt Northern frameworks and the enforcement of these frameworks is currently an even bigger question. Since 2019, several critical questions were raised regarding the NDPR, ranging from its legitimacy to inconsistent provisions, and a lack of compliance among federal agencies (Omotubora, 2021). Despite concerns regarding the practical effectiveness of NDPR and the eventual NDPA, debates regarding privacy legislation have been shaped throughout by references to Northern-produced legal frameworks and norms (Emmanuel, 2022).

For instance, a series of bills from 2009 to 2015 that acted as a precursor to the eventual NDPR highlighted several issues with transplanting Global North-inspired legislation into the Nigerian context: practical, social, and economic difficulties would prevent private citizens in Nigeria from effectively raising complaints regarding privacy rights violations; provisions relating to healthcare data that were copied from Global North legislation did not apply in the Nigerian context; and a draft privacy bill omitted public institutions from its remit because the bill was modeled on Canadian legislation which referred to a separate Privacy Act, which did not exist in Nigeria (Iwobi, 2017). Nonetheless, ‘legal transplantation’ from Global North contexts profoundly shaped the drafting and implementation of the NDPR and NDPA, even as critics argued against a ‘cut and paste’ approach to privacy and data protection law (Makulilo, 2013).

Regardless of its shortcomings, the NDPA could strengthen compliance and enforcement especially due to provisions on the Nigeria Data Protection Commission’s (NPDC) powers of arrest, search, seizure, forfeiture, fines, and prosecution (Sections 49 and 58, NDPA, 2023). However, with respect to intergovernmental enforcement of data protection, the exemption of public authorities from key provisions of the Act on the ground of ‘prevention, investigation and detention’ of crime already casts doubt on the political will of the government to hold its agencies accountable under the law (Section 3(2)(a)). Such exceptions mirror those found in Northern and international legislation on human rights, such as the ECHR’s exception to privacy rights on grounds of ‘national security, public safety or the economic wellbeing of the country’ under Article 8 (2). Legal researchers have noted and criticised the expansive nature of these exceptions in the context of digital surveillance (Margulies, 2013).

These international influences have interacted with the domestic political agency of institutions shaping the law and practice of data protection and enforcing privacy rights. In terms of enforcing data protection, especially in intergovernmental data breaches and incidents by state actors, public ombudsmen have thus far been ineffective. When curtailing the demands of privacy and data protection, public bodies in Nigeria have cited court decisions that subverted fundamental rights in favour of national security to suit their narratives even when the facts and circumstances of prior cases are unrelated

to the case at hand. One illustrative example is the Nigerian Immigration Service's (NIS) publication of a Nigerian citizen's international passport data page on social media without consequences (Diyoke and Edeh, 2020). In addition, between 2020 and 2021, the Lagos State Government and the NIS were culpable in data breaches of varying extents, but no strong sanctions were taken against these governmental bodies (Cybersecfill, 2019).

The NIS statutorily processes the data of millions of citizens and immigrants, yet its data protection and privacy consciousness are deficient. Both the NDPR and NDPA prescribe transparency of processing activities, the appointment of data protection officers, filing of annual compliance reports/audits, breach notifications, and reporting, but the NIS has not yet complied with any of these requirements. Neither the Immigration Act nor associated regulations discuss the right to privacy or data protection. Provisions on the 'presentation of travel documents' and the maintenance of an 'immigration registry' do not have corresponding provisions relating to the right to privacy and data protection. As we discuss in the next section, the NIS's poor rights-related track record has in fact empowered the IOM as an external rights 'expert' able to reshape the practices and technologies of digital surveillance at the border (Sokhi-Bulley, 2019). Such expertise, however, has been primarily used to promote the further expansion of digital border surveillance, according to the logics of 'crimmigration control' (Bowling and Westenan, 2018) – the merger of migration control with law enforcement practices – that are dominant in the Global North yet novel in the Nigerian context.

Coloniality of Sociotechnical Knowledge at Nigeria's Digital Borders

Postcolonial Dimensions of Territory and Mobility Control

The preceding discussion demonstrates how privacy legislation in Nigeria has been influenced by Northern-produced norms, which are promoted globally in the name of universal rights (An-Naim, 2021). Such ideas reshape juridical practice in a 'top-down' fashion as federal authorities enact new legislation that then influences practices on the ground to varying extents. Examining the co-production of law, society, and technology through and infra-legality approach brings into view how these legislative frameworks are also being shaped by 'bottom-up' dynamics of technological development. The deployment of new digital infrastructures at the Nigerian border can be critically analysed in terms of the coloniality of sociotechnical knowledge; epistemic inequalities determine who gets to set global technical standards and what kinds of technical practices are seen as reflective of 'modernisation' and 'progress'.

In recent decades, Nigerian federal authorities have relied on the digitalisation of the country's border control practices to assert their authority internally and demonstrate their statehood to external audiences (Singler, 2023). Since 2007, with the support of the IOM, the NIS has expanded its capacity to collect digital biometric data at the border and used these data to detect irregular passengers, criminals, and suspected terrorists through the deployment of the MIDAS system. The IOM offers MIDAS as a free technological 'solution' to its member states in the Global South, through projects funded primarily by

Global North states. The system is currently active in 20 states, most of which are on the African continent (IOM, 2018). Nigeria has the most extensive roll-out of the system thus far.

The development of digital surveillance capacities at the border has been decisively shaped by Northern-produced conceptions of state modernity as the capacity to effectively control cross-border mobility, as well as Northern technical standards relating to the extent and type of digital data collection and data sharing in border control contexts (Jegen, 2023). Externally, states must now demonstrate not only effective control of their borders, but more specifically their 'biometric statehood': their capacity to use digital biometric identification technologies to detect and identify border crossers (Muller, 2010).

Although MIDAS in Nigeria still suffers from technical limitations and is not yet connected to international policing databases such as Interpol's I-24/7 system, the country's federal officials already regularly show off the system to international delegations. For instance, in 2023 Nigeria's Minister of Interior demonstrated MIDAS to a delegation of security officials from other countries, stating that 'the NIS is now better equipped with advanced technology to curtail any breach in Nigeria's borders' (Akintaro, 2023). Such statements and demonstrations have been crucial to ensuring Nigeria's active involvement in regional and global political partnerships, despite experts and researchers arguing that the country's borders remain highly permeable (Ifeanyi-Aneke et al., 2021). Upholding international norms relating to border control contrasts with Nigeria's resistance to contemporary norms relating to same-sex marriage, demonstrating the strategic nature of performing statehood in selective ways according to local sociopolitical understandings and interests (Singler, 2021).

Meanwhile, the IOM and NIS have been preparing for the future expansion of MIDAS, in terms of establishing international connectivity and allowing for the collection and analysis of crime control- and security-oriented advance passenger information (API) and passenger name record (PNR) data in the future. API and PNR data represent more expansive and more sensitive forms of digital surveillance (Han et al., 2017). These forms of data require more robust privacy rights and data protection legislation, as well as institutional interagency practices between immigration control and law enforcement agencies. These requirements are determined by current global 'best practices' and international technical standards set by organisations such as the International Civil Aviation Organization (ICAO) and IOM (ICAO, 2010). During workshops and meetings with Nigerian federal officials relating to the planned expansion of international connectivity and sensitive data collection in 2021, IOM officials became concerned with the possibility that Nigeria's new data protection legislation might limit the opportunities for future expansive digital surveillance at the border.

Digital Colonialism and the 'Modernisation' of Border Control

The IOM explicitly positions its MIDAS border control technology as a 'modern' system capable of monitoring migration flows and identifying security risks at the border (IOM, 2023). In Nigeria, federal officials are also aware of the need to appear 'modern' in order to engage with the international system, and to this end, they reproduce the discourse of technological modernisation. In August 2023, the NIS Lagos State Zonal Coordinator

argued that the expansion of MIDAS in Nigeria is reflective of the federal government's willingness to 'embrace modern solutions that facilitate and secure border controls' (IOM, 2023).

These dynamics are representative of the coloniality of sociotechnical knowledge to the extent that technical norms and technological devices are primarily developed in Global North contexts, promoted globally by Northern-funded actors, and variously accepted, supported, contested, and translated by Global South actors. To speak of the coloniality of knowledge in this context is not necessarily to invoke the extractive logics of digital colonialism qua surveillance capitalism (Kwet, 2019; Zuboff, 2019). In fact, IOM officials are aware that by providing MIDAS free of charge, they are competing against capitalist logics of profit extraction and private gain. One official working in another MIDAS-operating country explained that the implementation of MIDAS faced pushback from private companies with existing digital systems at the border, and their clients in the state migration agencies. According to this official, these private companies 'weren't keen to discuss things with us, because they saw us as a potential threat [...] there is a flow of money which is very, very unclear' (Interview, 13 February 2021).

IOM officials partly view their role as protecting Southern states from getting locked into such economically detrimental arrangements with private companies: 'The idea [with MIDAS] was basically providing an alternative to private sector systems, which are often very expensive to purchase and which often also have this kind of buyer lock-in where states are then dependent on a private company, sometimes even for accessing the data that is stored in the systems' (Interview, 9 March 2021). Yet, despite the IOM helping states avoid the profit-oriented logics of the private sector, MIDAS in Nigeria can also be analysed in terms of digital colonialism to the extent that Northern-produced modernisation discourses underpin and legitimise the expansion of the system. The justification of 'improving' 'backward' peoples (Arneil, 2024) through pedagogical and technological interventions is evident when IOM officials describe MIDAS as 'a step forward' for African countries (Interview, 10 March 2021). Deployment of the system is not presented as a political choice that reflects a particular understanding of migration control; instead, refusal to use the technology is attributed to a 'lack of [awareness] of the potential of MIDAS' (Interview, 3 March 2021).

Leonie Jegen's (2023) analysis of the coloniality of knowledge in externally funded migration control interventions in Niger is instructive in terms of critically analysing the IOM's MIDAS in Nigeria as well. According to Jegen (2023), the coloniality of knowledge underpinning Niger's border control practices is reflected in two key dimensions that characterise capacity-building interventions there. First, 'the starting point' of political discourses relating to border control are Northern-produced norms and practices rather than local perspectives on mobility control (Jegen, 2023: 8). So too, in the Nigerian context, discussions regarding the deployment and expansion of MIDAS regularly refer to international standards, 'modernisation' and territorial conceptions of state authority, while local perspectives on mobility control are sidelined. The modern notion of territorial sovereignty, with clearly demarcated borders dividing national communities, clashes with the sociocultural and economic realities of cross-border communities across the border regions of Nigeria and its neighboring countries (Bosiakoh, 2019; Liman, 2018). IOM officials also refer to international standards as a justification for

interventions that might otherwise be conceptualised as violations of state sovereignty. In the context of developing new privacy rights legislation – which IOM officials wanted to ensure would include exceptions for national security and crime control efforts at the border – one official remarked: ‘Usually, it’s not the role of international organizations to draft laws for countries [...] but if we don’t do it, it’s just not going to happen’ (Field diary, 5 August 2021).

Second, it is not only external actors who reinforce and deploy Northern political discourses regarding border control; Southern actors are also ‘required to speak in order for their practices [...] to be classified along pre-defined categories [...] these categories are then reproduced in policy documents and national strategy papers’ (Jegen, 2023: 8). In Abuja, NIS officials reproduced the IOM’s discourses of MIDAS as a ‘modern’ form of border control and also of the IOM’s supposed status as a human rights ‘expert’ organisation, which justifies the organisation’s interventions in the country. At one IOM-led workshop in Abuja, an NIS official explained that ‘the IOM is our preferred partner, in many ways, because they are with the UN [...] and the UN set the standard for human rights’ (Field diary, 3 August 2021).

Local Contestation and Privacy Rights at the Digital Border

Highlighting the ‘post-imperial’ relationship between the IOM and its local interlocutors is not to reduce local agency to the reproduction of Northern discourses relating to privacy rights and mobility control (Singler, 2023). Nigerian federal agencies have actively shaped the IOM’s interventions in the country, and the deployment of MIDAS has been characterised by local political disputes and conflicting interests as well. Highlighting the impact of such agency provides a Southern perspective on our analysis of privacy rights and border control while contextualising Nigerian federal authorities’ agency against the backdrop of the coloniality of legal and sociotechnical knowledge.

Where cross-border traveler information was previously collected in analog form, and border control officers examined physical passport stamps and visas, MIDAS now analyses and stores such data in a digital format. The technical infrastructure of MIDAS has forced some institutional changes to immigration control in Nigeria, and these changes are characterised by local political contestation and friction. Within the NIS, one officer in Abuja explained that before MIDAS, many immigration control functions were previously decentralised to the local state level due to the practical difficulty of coordinating at the federal level. MIDAS, however, is meant to overcome these practical obstacles thanks to its (mostly) real-time connectivity to the central database at NIS headquarters in Abuja. State-level agencies have not always welcomed this centralisation of authority, but technical considerations have helped officials push through such changes nonetheless: ‘Of course they [local state authorities] do not always like it, but the MIDAS database is here in Abuja. So, they must send the data here. They cannot keep it to themselves’ (Field diary, 3 August 2021).

Another aspect of domestic political contestation relates to the IOM’s future plans to enable the ‘full capacity’ of MIDAS by enabling it to collect and analyse API and PNR data at the border. These forms of data are more sensitive, requiring robust data protection and privacy rights legislation. They are also more explicitly connected to the logics of

crime control and national security. According to ICAO (2010, Section 2.2.1), these forms of data are particularly important for 'the fight against terrorism and serious crime'. The merging of border control with the logics of crime control and national security has been extensively documented in several Global North states, with border criminologists now regularly referring to the expansion of 'crimmigration control' practices (Bowling and Westetra, 2018). In the context of digital border control databases, new digital systems are now regularly set up with shared access between immigration control and law enforcement authorities, while older systems that were initially developed for narrow immigration control purposes have later been expanded to allow law enforcement access as well (Dekkers, 2020).

In Nigeria, this merger of border control and law enforcement is historically novel. Both the NIS and the Nigeria Police Force, like other federal agencies, have historically guarded their institutional remits and have been hesitant to share responsibilities. Yet, according to international technical standards, connecting to international alert lists and processing API and PNR data require 'secondary inspection' mechanisms whereby data are shared between immigration authorities and law enforcement agencies (IOM, 2018). In Nigeria, setting up such interagency cooperation and requisite legal frameworks has been fraught with political difficulties. As one official from the Federal Ministry of Justice in Abuja explained: 'Setting up secondary inspection, this has been an issue for some time. We are ready, we know what are the critical agencies that are needed in secondary inspection [...] But this is a problem for them [NIS]' (Field diary, 28th July 2021).

In addition to such political difficulties, interagency cooperation in Nigeria has also raised concerns regarding data protection, privacy rights, and non-discrimination at the border. We explained above that the NIS does not possess a stellar track record when it comes to data protection regulations and requirements. The Nigeria Police Force, in turn, was ranked the 'most corrupt' public institution by the general public in a comparison of 34 African countries in 2015 (Olonisakin et al., 2018: 31). IOM officials are aware of potential privacy rights issues when expanding the functionality of MIDAS in the future. As one official put it in a meeting relating to API data collection: 'Sometimes national watchlists are not so robustly protective of individual rights. This will mean that expanding the system can be problematic in terms of data access' (Field diary, 5 August 2021).

Despite such potential concerns, however, the future expansion of MIDAS was often treated as a foregone conclusion, not least by putting in place technical infrastructures even in the absence of prior political agreements or robust privacy legislation. In Abuja, a computer station for Interpol connectivity was already set up at NIS headquarters in the summer of 2021, though the requisite legal frameworks for secondary inspection had not yet been developed (Field diary, 3 August 2021). API and PNR data collection were also presented by IOM officials as inevitable technical expansions of the system: 'MIDAS needs to collect API data, and API data is the foundation for processing PNR data' (Field diary, 5 August 2021). The IOM's technical expertise was combined with frequent mention of international standards and best practices to sideline political questions about the desirability and potential risks to privacy rights arising from expanded data collection at the border.

A central pillar of the IOM's expertise in meetings and workshops was the regular reference to concerns about the right to privacy and non-discrimination. Expansive data protection practices in border control contexts have been extensively criticised in the Global North precisely because they present new risks to individual rights. In Nigeria, however, the IOM deployed a rights-based discourse not to limit border surveillance practices but to legitimise their expansion by promoting the inclusion of security- and crime control-related exceptions in the NDPA. Although it is difficult to trace the influences between the IOM's API-related workshops and the final NDPA, the Act eventually included exceptions that are necessary for expansive border surveillance. According to Section 3(1) of the Act, it 'shall not apply to a data controller or data processor if the processing of personal data' is used for 'the investigation, detection, prosecution, or adjudication of a criminal offence' or 'as is necessary for national security'. The IOM is still actively involved in efforts to enable API and PNR data collection by MIDAS at the Nigerian border (IOM, 2022).

Ultimately, the IOM's technical and rights expertise has influenced Nigeria's emerging legal regime for data protection from the bottom up alongside the influence of top-down legal norms on the country's new Data Protection Act. Putting into place digital infrastructures has necessitated the development of regulatory frameworks and legal exceptions that have allowed federal officials to deploy these digital technologies and will allow them to expand their digital surveillance capabilities in the future. The IOM's human rights discourse maps onto postcolonial hierarchies that reflect the coloniality of legal knowledge, allowing Global North actors to 'teach' Nigerian authorities how to 'do' human rights properly even when such lessons do not result in more robust protections for individual rights in practice (Sokhi-Bulley, 2019). The dominant Northern understanding of digital borders as a matter of 'cimmigration control' acts as the 'starting point' for political debates regarding MIDAS and privacy rights in Nigeria (Jegen, 2023: 8).

Conclusion

In this article, we have critically analysed the coloniality of legal and sociotechnical knowledge underpinning the emergence of a new legal regime for privacy rights in Nigeria. We have demonstrated how enduring postcolonial epistemic hierarchies have influenced this legal regime in both top-down and bottom-up fashion. On one hand, the coloniality of legal knowledge is evident in how new federal legislation mirrors legal standards and frameworks set in the Global North. On the other hand, socio-technical developments at Nigeria's expanding digital borders – shaped by the technical expertise of the Northern-funded IOM – have exerted a bottom-up pressure on these legislative frameworks as well. Following the infra-legality approach (Sullivan, 2022), the case of Nigeria's emerging legal regime for data protection illustrates the utility of analysing legislative changes and lawmaking practices side by side with socio-material processes of digitalisation and the development of new technical infrastructures.

To be clear, our argument is not that privacy rights are somehow undesirable or that we should reject human rights entirely due to their colonial underpinnings. Instead, invoking the coloniality of knowledge relating to 'universal' human rights is meant to problematise

the privileged position claimed by Northern actors to determine how human rights should be conceptualised and what moral and technological ‘progress’ should look like. This analytical move is not meant to result in a rejection of human rights but rather a more nuanced understanding of how local agencies and interests also inform the process of translating universal rights into local contexts. In Nigeria, local sociocultural understandings of privacy and mobility and the practical realities of legal protection, digital competence, and border control have shaped both the enforcement of the Global North-inspired NDPA in action as well as the roll-out of the IOM’s MIDAS system. This article also highlights the importance of critically analysing whether the deployment of human rights discourse by Northern actors in Southern contexts is actually used to create more robust protections for individual privacy and other rights or instead used to formalise and normalise exceptions to them.

We have sought to add nuance to the scholarship on digital colonialism (Coleman, 2019; Kwet, 2019) by disentangling the coloniality of legal and sociotechnical knowledge from the extractive and dispossessive logics of transnational surveillance capitalism (Firmino et al., 2019; Zuboff, 2019). Even when profit-oriented data extraction and dispossession are not the central drivers of digitalisation and new data protection legislation in the Global South – and even when Southern actors themselves actively engage in the process of promoting such processes – postcolonial epistemic hierarchies can still shape understandings of rights in digital contexts.

The normative thrust of the arguments above is that it is imperative to decolonise and Southernise our understanding of privacy rights legislation in the context of digitalisation in the Global South. Doing so can highlight the enduring coloniality of legal and sociotechnical knowledge relating to privacy rights and digital surveillance. When deconstructing such coloniality, we should also avoid conceptualising Northern actors as the primary, or only, actors responsible for new legislation and practices in the Global South by reducing such practices to their post-imperial dimensions. Instead, the Southernisation agenda can productively expand upon decolonial analyses by highlighting the role of Southern actors in shaping Northern interventions and contributing to the creation of novel constellations of rights legislation and digital practices globally.


Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The authors received no financial support for the research, authorship and/or publication of this article.

ORCID iD

Samuel Singler  <https://orcid.org/0000-0001-6231-7095>

References

- Abdulrauf L and Daibu A (2016) New technologies and the right to privacy in Nigeria: evaluating the tension between traditional and modern conceptions. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 7: 113–124.
- Aho B and Duffield R (2020) Beyond surveillance capitalism: privacy, regulation and big data in Europe and China. *Economy and Society* 49(2): 187–212.
- Akintaro S (2023) FG says Nigerian Immigration Service is now better equipped with technology. Available at: <https://nairametrics.com/2023/03/10/fg-says-nigerian-immigration-service-now-better-equipped-with-technology/> (accessed 20 July 2023).
- Akintola SO and Akinpelu DA (2021) The Nigerian Data Protection Regulation 2019 and data protection in biobank research. *International Data Privacy Law* 11(3): 307–318.
- Aliverti A, Carvalho H, Chamberlen A, et al. (2021) Decolonizing the criminal question. *Punishment & Society* 23(3): 297–316.
- An-Naim AA (2021) *Decolonizing Human Rights*. Cambridge: Cambridge University Press.
- Arneil B (2024) Colonialism versus imperialism. *Political Theory* 51(1): 146–176.
- Arora P (2019) General Data Protection Regulation—a global standard? Privacy futures, digital activism, and surveillance cultures in the Global South. *Surveillance & Society* 17(5): 717–725.
- Babalola O (2021) The EU GDPR and Nigeria’s NDPR: A comparative analysis. *Journal of Data Protection & Privacy* 4(4): 372–387.
- Babalola O (2022) Nigeria’s data protection legal and institutional model: an overview. *International Data Privacy Law* 12(1): 44–52.
- Bosiakoh TA (2019) Nigerian immigrants as ‘liminars’ in Ghana, West Africa: narratives on mobility, immobility and borderlands. *Journal of Asian and African Studies* 54(4): 554–568.
- Bowling B and Westera S (2018) ‘A really hostile environment’: adiaphorization, global policing and the crimmigration control system. *Theoretical Criminology* 24(2): 163–183.
- Byrne WH, Gammeltoft-Hansen T and Stappert N (2023) Legal infrastructures: towards a conceptual framework. *MOBILE Working Paper Series* (33).
- Chimakonam J and Agada A (2020) The sexual orientation question in Nigeria: cultural relativism versus universal human rights. *Sexuality & Culture* 24(6): 1705–1719.
- Choroszewicz M and Mäihäniemi B (2020) Developing a digital welfare state: data protection and the use of automated decision-making in the public sector across six EU countries. *Global Perspectives* 1(1): 12910.
- Coleman D (2019) Digital colonialism: the 21st century scramble for Africa through the extraction and control of user data and the limitations of data protection laws. *Michigan Journal of Race & Law* 24(2): 417–440.
- Cybersecfill (2019) Breach of Nigeria Data Protection Regulation by LIRS. Available at: <https://www.cybersecfill.com/breach-of-nigeria-data-protection-regulation-by-lirs/> (accessed 5 January 2024).
- Dekkers T (2020) Technology driven crimmigration? Function creep and mission creep in Dutch migration control. *Journal of Ethnic and Migration Studies* 46(9): 1849–1864.
- Diyoke M and Edeh S (2020) An analysis of data protection and compliance in Nigeria. *International Journal of Research and Innovation in Social Science* 4(5): 377–382.
- Dobinson I and Johns F (2017) Legal research as qualitative research. In: McConville M and Chui WH (eds) *Research Methods for Law*. 2nd ed. Edinburgh: Edinburgh University Press, pp. 18–47.
- Emmanuel F (2022) A review of Digital Rights Lawyers Initiative v Unity Bank on approaching the administrative redress panel as a condition precedent to an action under the Nigeria Data Protection Regulation. *The Gravitas Review of Business & Property Law* 13(4): 66–72.

- European Union (2022) The EU–Nigeria Digital Economy Package (2021–2024). Available at: https://ec.europa.eu/commission/presscorner/api/files/attachment/871307/GG_Nigeria%20factsheet.pdf (accessed 15 December 2023).
- Feenan D (2013) Exploring the ‘socio’ of socio-legal studies. In: Feenan D (eds) *Exploring the ‘Socio’ of Socio-Legal Studies*. Basingstoke: Palgrave Macmillan, pp. 3–19.
- Firmino R, de Vasconcelos Cardoso B and Evangelista R (2019) Hyperconnectivity and (im)mobility: uber and surveillance capitalism by the Global South. *Surveillance & Society* 17(1/2): 205–212.
- Frowd PM (2024) The ‘datafication’ of borders in global context: the role of the International Organization for Migration. *Geopolitics*. DOI: 10.1080/14650045.2024.2318580.
- Han C-R, McGauran R and Nelen H (2017) API And PNR data in use for border control authorities. *Security Journal* 30(4): 1045–1063.
- Harvey WS (2011) Strategies for conducting elite interviews. *Qualitative Research* 11(4): 431–441.
- Hilal AYH and Alabri SS (2013) Using NVivo for data analysis in qualitative research. *International Interdisciplinary Journal of Education* 2(2): 181–186.
- Ibrahim AM (2015) LGBT rights in Africa and the discursive role of international human rights law. *African Human Rights Law Journal* 15: 263–281.
- ICAO (2010) *Guidelines on Passenger Name Record (PNR) Data*. Montreal: ICAO.
- Ifeanyi-Aneke F, Ifedi F and Aga S (2021) Nigeria Immigration service and the challenge of cross border human trafficking in Nigeria 2011–2019. *University of Nigeria Journal of Political Economy* 11(1): 124–134.
- IOM (2018) MIDAS: a comprehensive and affordable Border Management Information System. Available at: https://acbc.iom.int/sites/default/files/2019-11/midas-brochure18-v7-en_digital-2606_1.pdf (accessed 10 April 2021).
- IOM (2022) The United Nations partners with the Federal Government of Nigeria on the establishment of an Advance Passenger Information and Passenger Name Record system. Available at: <https://nigeria.iom.int/news/united-nations-partners-federal-government-nigeria-establishment-advance-passenger-information> (accessed 10 March 2023).
- IOM (2023) IOM hands over MIDAS equipment to the Nigeria Immigration Service. Available at: <https://nigeria.iom.int/news/iom-hands-over-midas-equipment-nigeria-immigration-service> (accessed 18 December 2023).
- Iwobi AU (2017) Stumbling uncertainly into the digital age: Nigeria’s futile attempts to devise a credible data protection regime. *Transnational Law & Contemporary Problems* 26(1): 14–61.
- Jasanoff S (2004) The idiom of co-production. In: Jasanoff S (ed) *States of Knowledge: The Co-Production of Science and Social Order*. Abingdon: Routledge, 1–12.
- Jegen LF (2023) ‘Migratising’ mobility: coloniality of knowledge and externally funded migration capacity building projects in Niger. *Geoforum; Journal of Physical, Human, and Regional Geosciences* 146: 103862.
- Kalu U and Ewuzie M (2021) Fundamental rights protection vis-a-vis application of limitation clause in the 1999 Constitution of Nigeria. *International Review of Law and Jurisprudence* 3(3): 184–189.
- Kilkelly U (2003) The right to respect for private and family life: a guide to the implementation of Article 8 of the European Convention on Human Rights. *Human Rights Handbooks, No. 1*.
- Kollman K and Waites M (2009) The global politics of lesbian, gay, bisexual and transgender human rights: an introduction. *Contemporary Politics* 15(1): 1–17.
- KPMG (2019) The Nigeria Data Protection Regulation: journey to compliance. Available at: <https://assets.kpmg.com/content/dam/kpmg/ng/pdf/advisory/NDPR-journey-to-compliance.pdf> (accessed 30 August 2024).
- Kwet M (2019) Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class* 60(4): 3–26.

- Lee M, Natarajan L, Lock S, et al. (2018) Techniques of knowing in administration: co-production, models, and conservation law. *Journal of Law and Society* 45(3): 427–456.
- Liman A (2018) The role of socio-cultural factors in informal cross-border flows between borderland communities of Nigeria and Niger Republic: the case of Illela-Birni N’konni international border communities. *Pakistan Journal of Humanities and Social Sciences* 6(2): 248–262.
- Linos K and Carlson M (2017) Qualitative methods for law review writing. *University of Chicago Law Review* 84(1): 213–238.
- Makulilo AB (2013) Data protection regime in Africa: too far from the European ‘adequacy’ standard? *International Data Privacy Law* 3(1): 42–50.
- Margulies P (2013) The NSA in global perspective: surveillance, human rights, and international counterterrorism. *Fordham Law Review* 82(5): 2137–2168.
- Martins BO and Jumbert MG (2022) EU Border technologies and the co-production of security ‘problems’ and ‘solutions’. *Journal of Ethnic and Migration Studies* 48(6): 1430–1446.
- Mawani R, et al. (2021) Postcolonial legal studies. In: Valverde M, Clarke K and Darian-Smith E (eds) *The Routledge Handbook of Law and Society*. Abingdon: Routledge, pp. 47–52.
- Muller B (2010) *Security, Risk and the Biometric State: Governing Borders and Bodies*. Abingdon: Routledge.
- NITDA (2020) Nigeria Data Protection Regulation performance report 2019-2020. Available at: [https://ndpc.gov.ng/Files/NDPR%20\(Lite\)%20Performance%20Report%20%202019-2020.pdf](https://ndpc.gov.ng/Files/NDPR%20(Lite)%20Performance%20Report%20%202019-2020.pdf) (accessed 17 December 2023).
- Nnamani SO (2011) Institutional mechanisms for human rights protection in Nigeria: an appraisal. *Nnamdi Azikiwe University Journal of International Law and Jurisprudence* 2: 128–137.
- Olonisakin T, Ogunleye A and Adebayo S (2018) The Nigeria criminal justice system and its effectiveness in criminal behaviour control: a social-psychological analysis. *International Journal of Accounting Research* 3(6): 28–44.
- Omotubora A (2021) How (not) to regulate data processing: assessing Nigeria’s Data Protection Regulation 2019 (NDPR). *Global Privacy Law Review* 2(3): 186–199.
- Oyedemi TD (2020) Digital coloniality and ‘next billion users’: the political economy of the Google Station in Nigeria. *Information, Communication & Society* 24(3): 329–343.
- Pharaon F (2023) Unleashing sustainable digital transformation in Nigeria. Available at: <https://www.ericsson.com/en/blog/1/2023/unleashing-sustainable-digital-transformation-in-nigeria> (accessed 15 December 2023).
- Quijano A (2000) Coloniality of power and Eurocentrism in Latin America. *International Sociology* 15(2): 215–232.
- Quijano A (2007) Coloniality and modernity/rationality. *Cultural Studies* 21(2–3): 168–178.
- Saleh-Hanna V (2008) *Colonial Systems of Control: Criminal Justice in Nigeria*. Ottawa: University of Ottawa Press.
- Singer S (2021) Biometric statehood, transnational solutionism and security devices: The performative dimensions of the IOM’s MIDAS. *Theoretical Criminology* 25(3): 454–473.
- Singer S (2023) Performativity, pragmatism and border control technologies: Democratising the ontologies of border criminology. *International Journal for Crime, Justice and Social Democracy* 12(2): 13–24.
- Singer S (2024) ”Do It Yourself!“ Pedagogical performances, technical expertise, and crimmigration control in the IOM’s capacity-building practices in Nigeria. *Geopolitics*. DOI: 10.1080/14650045.2024.2331802.
- Sokhi-Bulley B (2019) *Governing (Through) Rights*. Oxford: Hart.
- Sullivan G (2022) Law, technology, and data-driven security: infra-legalities as method assemblage. *Journal of Law and Society* 49(S1): S31–S50.

- Tabiu M, et al. (2001) National Human Rights Commission of Nigeria. In: Hossain K, Besselink L and Selassie HSG (eds) *Human Rights Commissions and Ombudsman Offices: National Experiences throughout the World*. Nijhoff: Brill, pp. 553–559.
- Thym D (2008) Respect for private and family life under article 8 ECHR in immigration cases: a human right to regularize illegal stay? *International and Comparative Law Quarterly* 57(1): 87–112.
- Ugwudike P (2020) Digital prediction technologies in the justice system: the implications of a ‘race-neutral’ agenda. *Theoretical Criminology* 24(3): 482–501.
- Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.
- Zumbansen P (2019) Transnational law as socio-legal theory and critique: prospects for ‘law and society’ in a divided world. *Buffalo Law Review* 67(3): 909–960.

Cases cited

- J. S. Olawoyin v. Attorney-General, Northern Region, Nigeria, 1960.
- Shugaba Abdulrahman Darman v. The Federal Minister of Internal Affairs and Others, Nigeria, 1980.
- Uchechi Nwachukwu v. Henry Nwachukwu & Anor, Nigeria, 2018.

Statutes cited

- Nigeria Data Protection Act (NDPA), 2023.