



## Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice

Isaac Juma & Bukola Fatureti

**To cite this article:** Isaac Juma & Bukola Fatureti (23 May 2025): Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice, International Review of Law, Computers & Technology, DOI: [10.1080/13600869.2025.2506918](https://doi.org/10.1080/13600869.2025.2506918)

**To link to this article:** <https://doi.org/10.1080/13600869.2025.2506918>



© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 23 May 2025.



[Submit your article to this journal](#)



Article views: 800




[View related articles](#)



[View Crossmark data](#)

# Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice

Isaac Juma<sup>a</sup> and Bukola Faturoti <sup>b</sup>

<sup>a</sup>Newcastle Law School, Newcastle University, Newcastle Upon Tyne, United Kingdom; <sup>b</sup>Hertfordshire Law School, University of Hertfordshire, Hertfordshire, United Kingdom

## ABSTRACT

As digital transformation accelerates across Africa, the need for effective data protection frameworks is increasingly urgent. The African Union's Digital Transformation Strategy (2020–2030) calls for harmonised legal and institutional measures to protect personal data and privacy rights. Yet, in practice, enforcement remains inconsistent, hindered by limited capacity, fragmented regulation, and low public awareness. This article presents a comparative analysis of data privacy enforcement in Kenya and Nigeria, focusing on the Data Protection Act 2019 and the Nigeria Data Protection Act 2023, respectively. It examines the roles of the Office of the Data Protection Commissioner and the Nigerian Data Protection Commission, particularly their institutional strengths and challenges. Using a qualitative approach, the study evaluates legislation, enforcement practices, and organisational structures, supported by case examples and regulatory outcomes. The findings indicate that Kenya has achieved measurable progress in data protection enforcement whereas Nigeria is still grappling with foundational issues. Despite these contrasts, both countries show alignment with global data protection norms such as the GDPR, offering a foundation for growth. The paper recommends targeted strategies to reinforce enforcement, including increasing institutional autonomy, expanding public education efforts, and building stronger technical capacity.

## KEYWORDS

Data protection; Nigeria; Kenya

## 1. Introduction

In the era of global digital transformation, the proliferation of personal data and its exploitation by public and private actors have underscored the urgent need for robust data protection frameworks. Internationally, the adoption of comprehensive data protection laws – anchored in principles enshrined in frameworks such as the EU General Data Protection Regulation (GDPR) – has fostered a trend toward legal harmonisation and regulatory convergence. This global momentum is further sustained by a shift toward stricter enforcement and the imposition of heavier penalties for data-related violations (Curtiss 2018).

**CONTACT** Isaac Juma  I.Juma2@newcastle.ac.uk

© 2025 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

Africa is increasingly part of this normative shift. As of January 2024, 36 of the 55 African Union (AU) member states (65%) have enacted comprehensive data protection laws. Three additional countries – Ethiopia, Namibia, and Malawi – have draft bills under consideration, while 16 countries still show no legislative progress in this domain. Significantly, one-third of all data protection laws in Africa have been passed within the last five years, signalling a rapid acceleration in legislative activity. Whereas 75% of Francophone African and 73% of Southern African countries have data protection laws, only 54% have their data protection legislation. Despite this legislative surge, the region continues to struggle with institutional weaknesses, regulatory fragmentation, and limited enforcement capacity.

The African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), adopted in 2014, uniquely shapes Africa's data governance landscape (African Union 2014). Though ratified by only 15 countries as of 2024,<sup>1</sup> it remains the world's only regional treaty to consolidate cybersecurity, electronic transactions, and data protection under a unified legal instrument. Its provisions represent a continental aspiration for harmonised digital governance, even as ratification delays have stalled implementation.

Fundamentally, digital transformation across top economies is regarded as a show of delivery on the government's mandate. Strategically, this technology has been leveraged to improve governance, financial services, and service delivery.<sup>2</sup> By the end of 2023, approximately 44% of the population in sub-Saharan Africa were mobile service subscribers, totalling 527 million users. Meanwhile, mobile internet penetration continued to grow, reaching 27% across the region by the end of the year (GSMA 2024).<sup>3</sup> The figure is expected to grow exponentially by 2030 since the new wave of technological uptake has facilitated the proliferation of digital hubs across Africa, with Kenya and Nigeria emerging as frontrunners.

Among the continent's most dynamic digital economies are Kenya and Nigeria. Often hailed as the Silicon Savannah, Kenya spearheaded digital financial innovation through platforms such as M-Pesa, fundamentally transforming mobile payments and digital commerce. Nigeria, Africa's largest economy by GDP and population, has cultivated a robust digital services sector, with Lagos emerging as a pan-African hub for fintech, health tech, and data-driven enterprises. These countries are witnessing exponential growth in the collection and processing of personal data, particularly within the spheres of e-commerce, online lending, mobile banking, and digital identity systems. The regulatory response in these two jurisdictions has been relatively recent. Kenya passed its Data Protection Act in 2019, creating the Office of the Data Protection Commissioner (ODPC), while Nigeria enacted the Nigeria Data Protection Act (NDPA) in 2023, establishing the Nigeria Data Protection Commission (NDPC). These legislative moves mark a significant shift from prior fragmented approaches to a unified legal regime. Yet, implementation remains an open question. Both countries are at an early stage of enforcement, grappling with institutional design limitations, resource constraints, regulatory fragmentation, and public awareness deficits.

While their legal frameworks exhibit ambition and alignment with global best practices – particularly around principles such as data minimisation, purpose limitation, and rights of data subjects – the real test lies in enforcement. Scholars such as Quach, Thaichon, and Martin (2022) caution that the benefits of comprehensive legislation can be undermined by weak enforcement, limited autonomy of regulators, and the absence of meaningful redress mechanisms. Furthermore, balancing digital innovation with rights-based data governance remains a key tension.

This article undertakes a comparative assessment of privacy enforcement in Kenya and Nigeria. It investigates how their respective frameworks and institutions respond to the complex challenge of safeguarding data rights in the context of accelerating digitalisation. The article is guided by three lines of enquiry, namely (i) How comprehensive and responsive are the legal frameworks in addressing emerging data protection challenges? (ii) To what extent are the ODPC and NDPC institutionally empowered to fulfil their enforcement mandates? and (iii) What policy, institutional, or structural reforms are necessary to advance privacy rights and ensure regulatory effectiveness? This paper aims to contribute to broader global debates on privacy enforcement in the Global South. It highlights how countries navigating digital expansion must innovate regulatory mechanisms that protect individual rights without stifling growth – an imperative for sustainable and rights-respecting digital development in Africa.

Regarding its structure, Part 2 of the paper explores the legal and institutional framework for data protection in Kenya and Nigeria. After this, Part 3 turns to the institutional capacities and enforcement approaches in Kenya and Nigeria, with an analysis of the agencies' interventions. Part 4, having offered an outlook on the challenges and opportunities and explored the potential avenues of bolstering the relevant frameworks, the article concludes with a summary of the findings and offers insights into possible key policy reforms identified as best practice. Furthermore, assessing the effectiveness of each country's legal frameworks, institutional design, and enforcement approaches delves into the broader socio-political and economic factors at the core of the realisation of a coherent data privacy framework. The final part reflects on opportunities for strengthening data protection in both jurisdictions and proposes policy interventions aligned with international good practices.

## **2. Legal framework for privacy enforcement in Kenya and Nigeria**

### ***2.1. Context of privacy enforcement in Kenya***

The proliferation of mobile technologies, epitomised by the use of mobile payment platforms, has been key to granting Kenya the leadership position in the continental tech landscape. However, as Kenya's tech sector grew, the legal framework for protecting personal data lagged. Efforts to create a robust framework for data protection were marked by weak and contradictory provisions on data and information privacy. This was partly credited to the fact that the privacy protection regime was spread across different legislation.

These piecemeal frameworks included three Acts that sought to protect privacy and two that sought to limit privacy. First of the three was the Kenya Information and Communications Act, which regulated the telecommunication sector by prohibiting the interception of messages or disclosing intercepted messages by licensed telecommunications operators, reinforced by the Consumer Protection Regulations 2010.<sup>4</sup> Second, the HIV and AIDS Prevention and Control Act 2006 embodies guidelines as prescribed by the Minister of Health, including identifying code related to the recording, collecting, storing and security of information, records or forms used in respect of HIV tests and related medical assessments.<sup>5</sup> Third, the Credit Reference Bureau Regulations, which regulated the submission of both positive and negative performance (credit reporting) of the

credit facilities extended to customers, incorporated mandatory requirements applicable to persons collecting, storing, submitting, or processing any data or information obtained under the provisions of the Regulations.<sup>6</sup> On the other hand, those that sought to limit an individual's privacy were the Prevention of Terrorism Act of 2012 and the National Intelligence Service Act of 2012.<sup>7</sup>

Early key developments leading to the current framework can be traced to the period before the adoption of the East African Community's (EAC) guidelines on the Reform of Cyber Laws (UNCTAD 2012).<sup>8</sup> In 2009, the Kenya Ministry of ICT issued a draft of the Data Protection Bill. This Bill did not meet the standards prescribed in the regional EAC framework.<sup>9</sup> Understandably, it was narrow in scope, having failed to address the responsibilities of data processors in the private sector. In the following year, Kenya adopted a constitution that explicitly provided for the right to privacy and its protection.<sup>10</sup> Despite this, all post-enactment efforts of bills relating to data protection were unsuccessful until 2018.

The emergence of the Data Protection Act 2019 represents a significant turnaround for data protection in Kenya. The legislation resolves the haphazard approach to data protection by consolidating all the provisions in the piecemeal data protection regime, with the preexisting legislation supplementing the current framework. Also, its coverage extends to the processing of personal data by both public and private bodies through automated or non-automated means.<sup>11</sup> The rights a citizen may exercise range across various handling processes, empowering data subjects and ensuring that data processors and controllers respect the individual's autonomy.<sup>12</sup> However, it exempts processing being undertaken by an individual during a purely personal or household activity if national security and public interest are deemed necessary and where disclosure is required by written law or court order.<sup>13</sup> It is worth noting the influence of the EU's GDPR. For example, the Kenya Data Protection Act (DPA) adopts terminology and concepts similar to the GDPR, including data subjects, processors, and controllers. It also mandates obtaining 'express, explicit, unequivocal, free, specific, and informed consent' before processing personal data.

Complementary to the DPA, the Ministry of Information, Communication and Digital Economy gazetted a task force to develop subsidiary legislation.<sup>14</sup> The ensuing framework included, firstly, the General Regulations 2021, which sets out the procedures for enforcing the rights of the data subjects and elaborating on the duties and obligations of the data controllers and data processors. Secondly, the Registration of Data Controllers and Data Processors Regulations 2021 sets out the procedures that the Office of the Data Commissioner will adopt in registering data controllers and data processors. Finally, the Complaints Handling and Enforcement Procedures Regulations 2021 outlines the complaints handling procedures and enforcement provisions for non-compliance.

## **2.2. Legal framework for privacy enforcement in Nigeria**

Nigeria, hosting one of Africa's largest economies and positioned as a centre of innovation, e-commerce and telecommunications, similarly lacked a dedicated and comprehensive data protection law before 2023. Data privacy was governed by various laws that provided partial protection. The precursor to the NDPA framework was embodied in the Nigeria Data Protection Regulation (NDPR), which sought to consolidate the existing piecemeal framework.<sup>15</sup> Before the NDPR, the privacy regulatory landscape of Nigeria was complex, with the country favouring sector-specific regulations while various efforts to have cohesive

and comprehensive legislation failed (Babalola 2022). For example, the National Information Technology Development Agency (NITDA) Act, the Nigerian Communications Commission (NCC) guidelines, and the Central Bank of Nigeria (CBN) failed to comprehensively address the digital privacy challenges posed by an increasingly interconnected community.

Till the enactment of the NDPA, the NDPR occupied a significant position as it outlined the legal requirements for data collection, storage and processing, paving the way for the NDPA framework. Under the NDPR framework, data protection compliance was supervised by the Nigeria Data Protection Bureau (NDPB), under the jurisdiction of the National Information Technology Development Agency (NITDA).<sup>16</sup> Although the NDPR was presented as a solution towards a robust data privacy framework, it was of limited force. It was a mere guideline rather than a formalised legal framework since it was issued by NITDA under its existing legal mandate rather than through an Act of Parliament. Furthermore, the absence of a formalised institutionalised structure for privacy enforcement brought about resistance based on a lack of statutory powers and capacity to implement the NDPR.<sup>17</sup> According to (Salami 2020), the NDPR's sparse, vague, and insufficient provisions create additional obstacles to compliance. Thus, the framework was incapable of addressing the challenges that rapid digital transformation presented in safeguarding personal data since it was a guideline rather than a statute.

### ***2.3. Analysis of the scope of legislation***

As the digital economy relies increasingly on data flows, provisions on data transferability are key to the integration of Kenya and Nigeria, which is particularly important in determining growth and positioning worldwide. Multinational firms operating in both countries and local firms with an international reach must comply with cross-boundary data-related obligations. The DPA controlling data transfers to third countries, states that transfers are only to be executed when adequate safeguards are in place to ensure the protection of data.<sup>18</sup> On the other hand, the scope of the NDPA is a significant shift from the approach enshrined in the NDPR. With revamped enforceability, particularly in cross-border transfer, the enhancement of the NDPC to protect its citizens' data serves as a critical step to curbing foreign mishandling of data.<sup>19</sup>

On agency provisions, the establishment of respective autonomous regulatory agencies represents a crucial step towards effective enforcement since the agencies are at the core of operationalisation of the data protection laws. The two privacy enhancing frameworks established independent authorities tasked with overseeing compliance, investigating violations, and issuing guidelines. Moreover, the agencies have the power to impose administrative fines and penalties for non-compliance in instances of infringement. This serves as a critical improvement in Nigeria since the autonomy is essential to the restriction of bureaucratic interference, which plagues independent agencies in the Global South (Jordana, Levi-Faur, and Fernández-i-Marín 2011). However, the regulatory capacity of both the ODPC and the NDPC remain a concern as subsequent sections analysing the structure and enforcement approaches will highlight.

Since Warren and Brandies published their seminal work on 'the right to privacy', the notion of the law protecting individuals from unwarranted intrusion even in the absence of physical harm evolved significantly to influence privacy laws worldwide (Warren and

Brandeis 1890). Following the norm, provisions in the Acts confer rights on data subjects. Granting individuals controlling powers over their personal data, the Acts mandate that data controllers and processors must obtain consent from individuals prior to handling of personal data, aimed at the prevention of unauthorised use of personal data, particularly by private corporations that actively engage in data mining for marketing and commercial purposes.<sup>20</sup> The provisions on consent align with the benchmark GDPR principle on consent being freely given, specific, informed, and unambiguous.<sup>21</sup> However, in both jurisdictions, the practical implementation of these rights poses a significant challenge since many citizens are unaware of their data protection rights and the possible redress available upon infringement. Furthermore, the context of consent poses unique challenges to the wider population, where the gap in the level of digital literacy complicates the practical realisation of 'informed consent.' With the rural population being highly marginalised, the probability of giving consent without understanding the implications complicates assessing the effectiveness of a consent-reliant data protection framework, particularly in the Global South (Radovanović et al. 2020).

In the sphere of data processors and controllers, the legislative frameworks impose specific obligations on data handlers requiring them to implement appropriate technical and organisational measures to protect personal data.<sup>22</sup> The measures, including encryption, regular security audits, and breach notification requirements, are complemented with accurate records of any data processing activities undertaken. Moreover, the regulatory agencies can inspect the adequacy of safeguards implemented by the handling parties. In cross-border transfers, the measures may involve the assessment of available comparable data protection law in the targeted country, and alternatively, having contractual clauses ensuring data protection.<sup>23</sup> However, the monitoring and enforcement of these provisions remains limited and will be determined by the ongoing scaling up of the agencies' resources and enforcement. Furthermore, the compliance costs of local firms may prove to be overbearing for small to medium-sized enterprises. This will be determined by the entities' capacity to implement technical and organisational measures to comply with the data handling obligations, largely influenced by access to financial and technical resources.

### **3. Institutional structures and enforcement trends in Kenya and Nigeria**

#### ***3.1. Trends in privacy enforcement in Africa***

Various data protection authorities have actively instituted regulatory measures ranging from enforcement notices to cease further processing or rectification to penalty notices awarded across the continent, highlighting significant data privacy fines issued by enforcers in the year 2023. Notable actions include the efforts of Agência de Proteção de Dados (APD), Angola's DPA, fining Africell \$150,000 for failing to get prior authorisation for data processing (Agência de Protecção de Dados 2024). Second, the ODPC had significant determinations impacting institutions spanning the lending sector, education, entertainment, digital identity, and digital currencies.<sup>24</sup> However, despite having issued the highest number of determinations, the combined value of the fines in Kenya was approximately \$124,700. In Nigeria, banks and institutions were fined over ₦ 350,000,000 for data privacy violations (NDPC 2023).<sup>25</sup> Finally, in South Africa, the Information Regulator issued a single



infringement notice imposing a \$279,000 fine against the Department of Justice and Constitutional Development for breaches of the Protection of Personal Information Act.<sup>26</sup>

### ***3.2. Institutional structures and enforcement mechanisms***

The assessment of the institutional approaches to regulation is done considering that the agencies are in their infancy and therefore a comprehensive analysis would be premature. However, it is possible to point out strengths that could be leveraged or weaknesses inherent in the overall enforcement framework. The ensuing assessment delves into the distinctive approaches to upholding data protection that lie in the legal instruments through which privacy enforcement is governed.

The KPDA is a comprehensive legislative framework, reflecting deliberate efforts to embed data protection within a single formal legal apparatus rather than a piecemeal framework. On the other hand, the NDPA showcases a renewal of efforts in data protection as it replaced a short-lived regulatory approach which lacked parliament-backed legislation. Analytically, with the need to strike a balance between efficiency and legitimacy, the prior regulatory approach profoundly affected the enforceability and the legitimacy of measures undertaken by the enforcement agency when addressing powerful entities who challenged its binding nature (Kosti, Levi-Faur, and Mor 2019). The subsequent move to a comprehensive legal framework signalled the gravity of the need for a legitimate and enforceable system. This is evidenced in the fact that parliament-backed legislations carry greater weight as it provides clarity in the form of a statutory authority like the ODPC and NDPC.

Furthermore, the legislative versus regulatory distinction frames the broader discourse on governance in Global South countries. The choice to enshrine privacy protection within law aligns the DPA and the NDPA with internationally established practice geared towards promoting legal certainty and stronger accountability mechanisms.<sup>27</sup> While expedient, a regulation-based approach that relies heavily on flexibility primarily serves short-term interests, potentially undermining long-term sustainability and the broader goal of establishing the jurisdiction as a global leader in data governance. Furthermore, the absence of a comprehensive statutory foundation necessary for effective enforcement creates a significant gap in addressing state-sanctioned surveillance and corporate misconduct. As the influential theory of responsive regulation suggests, a legislative framework strengthens the resilience of regulatory regimes and enhances their capacity to enforce provisions rigorously, thereby withstanding political and corporate pressures (Ayres and Braithwaite 1992; Braithwaite 2011).

Significantly, the enforcement powers granted to the regulatory authorities are at the core of establishing a culture of compliance, particularly those in the telecommunications, fintech, and healthcare, where personal data facilitates access to services (Dongyeon Kim et al. 2019; Kshetri 2016; Romanosky and Acquisti 2009)<sup>28</sup> Investigatory powers, which are essential for determining breaches and imposing penalties, are often triggered by the lodging of complaints. Nonetheless, regulatory agencies are also mandated to initiate investigations in response to concerns arising from sector-specific practices. In the Kenyan context, handling complaint-based investigations illustrates the Office of the Data Protection Commissioner's (ODPC) proactive approach, as it commits to assessing and resolving complaints within a 90-day timeframe.<sup>29</sup> On the other hand, the NDPC's



approach lacks specificity in terms of time limitation, with the general guidance stating that the communication of a decision shall be within 45 days of holding a pre-action conference.<sup>30</sup> It remains to be known how long after complaints the pre-action conference is to be held, and the length of the investigation by the authority, thus shrouding the entire process in obscurity. Ideally, the NDPC's approach ought to be consolidated by further guidance on the total period to carry out investigations and communication of a decision, geared towards ensuring lagging in enforcement is not tolerated.

As a key source of funding for the agencies, the fining mechanism is key to the enforcement framework, with the agencies' ability to impose administrative fines utilised to push for compliance (Balch 1980; Grant and Crowther 2016).<sup>31</sup> In the Kenyan framework, the Commissioner can impose fines of up to KES 5,000,000 or 1% of the company's annual turnover, whichever is lower.<sup>32</sup> A stark contrast to GDPR provisions in terms of amount, the fines reflect the significance of contextualisation of the framework, considering the socio-economic status of the entities in Kenya. However, the fines are insubstantial in the current framing of the provisions upon the determination of infringement. This results from the inclusion of the clause 'whichever is lower,' compounded by a lack of specificity on the turnover assessment, severely impacting the efficacy of the administrative fine mechanism. The severity of the provisions would be unquestionable, whereas the ODPC administrative fine determination would tip towards the higher scale rather than the alternative, to effectively deter infringement.

Case in point, the risk of undermining enforcement through current provisions may take the form of a processor or controller's recurrent infringement, considering the fines as an operating cost to be financed in the long run in light of possible benefits arising from the conduct (Baldwin 1995; Grant and Crowther 2016). The current enforcement framework appears vulnerable to potential shortcomings, particularly regarding the effectiveness of administrative penalties. If the provisions remain unchanged, introducing a specified daily fine for ongoing infringements could enhance the efficacy of the fine mechanism. Conversely, the existing limitations on administrative fines may be intentionally designed to avoid overburdening small and medium-sized enterprises with compliance costs. However, if this is indeed the rationale, it significantly undermines the normative strength of the Data Protection Act (DPA), as such a framework inadvertently privileges large national or multinational corporations. As a result, the DPA should reconsider its provisions, as the current approach has led to a prevalence of minimal administrative penalties with limited deterrent impact on non-compliance.

In Nigeria, the penalty mechanism under the Nigerian Data Protection Act (NDPA) demonstrates a more nuanced and structured approach, addressing gaps evident in Kenya's Data Protection Act (DPA). The Nigerian Data Protection Commission (NDPC) adopts a tiered framework that distinguishes between small to medium-sized enterprises and large corporations. This classification creates a functional taxonomy by categorising data controllers as either of 'major importance' or 'not of major importance.' Entities deemed to be of major importance are subject to penalties of ₦10,000,000 or 2% of their annual gross revenue – whichever is higher – while those not classified as such face a reduced fine of ₦2,000,000. Although the administrative fines may appear modest in absolute terms, the NDPA's emphasis on a percentage of turnover and application of the greater amount signals a stronger commitment to proactive and proportionate regulation, in stark contrast to the Kenyan model. Crucially, the strength of the

Nigerian framework lies in its enforcement efficacy, with a lower risk of both over- and under-enforcement, thereby enhancing its deterrent effect.

### **3.3. Privacy enforcement in action**

The regulation of online digital lenders and their data handling practices has emerged as a central concern for data protection authorities across the African continent. In this context, both Kenya and Nigeria have adopted active oversight roles. Kenya's Office of the Data Protection Commissioner (ODPC) approved at least 32 lenders from over 400 applications, while Nigeria approved a minimum of 203 digital lenders, with 38 under conditional approval and 47 subsequently delisted. The ODPC has placed significant emphasis on ensuring substantive compliance with the Data Protection Act (DPA), signalling its intent through vigorous enforcement measures. This commitment is reflected in the issuance of at least three penalty notices and five enforcement notices, alongside a targeted audit campaign involving 40 digital lenders. These actions were prompted by the receipt of over 1,000 complaints, of which 54 per cent of the 555 formally admitted cases related specifically to digital lending practices.<sup>33</sup>

For instance, in the consolidated complaints against Mulla Pride Ltd, six complaints were received against the respondent within a span of 40 days between the dates of 29th Sept 2023 and 7th Nov 2023.<sup>34</sup> The ODPC assessed and consolidated complaints on the respondent's bombardment of the complainants with texts and phone calls demanding payment of loans awarded to unknown parties. Furthermore, complainants were threatened the bombardment would only get worse. The ODPC upon the assessment of the evidence submitted was to determine whether the respondent fulfilled its duty to notify the complainants of the use of their contact details; whether there was an infringement; and whether the complainants are entitled to any remedies. Subsequently, the Commissioner held the respondent liable and issued an enforcement notice with a fine of KES 2,975,000.

In Nigeria, there have been over 400 reported cases of privacy breaches involving digital lending platforms. In response to these abuses, many platforms have cooperated with the Nigerian Data Protection Commission (NDPC) in implementing corrective and deterrent measures. By the end of 2023, approximately 203 lending platforms had been approved, while 47 were delisted, demonstrating a growing commitment to embedding data protection principles within digital lenders' policies and operations.<sup>35</sup> Although detailed documentation of individual cases remains limited, the NDPC's 2023 annual report briefly highlights key enforcement actions. Notably, insights can be drawn from a reconstructed case involving a complainant, Mr FredFide, which illustrates the Commission's regulatory approach towards digital lenders. In this instance, after defaulting on a loan, the complainant was subjected to threats of public embarrassment by the lender, aimed at compelling immediate repayment. The lender subsequently accessed the complainant's mobile device and unlawfully disseminated confidential information, resulting in significant personal humiliation. Upon receiving the complaint, the NDPC invited the respondent to a pre-action conference, during which the firm denied operating as a lending entity and disclaimed any association with the phone numbers used to contact the complainant. This case underscores the intrusive practices often employed by digital lenders and highlights the urgent need for robust organisational mechanisms to facilitate accessible complaint resolution and redress for data subjects.

## 4. Placing the law in context: challenges and promises

### 4.1. Conceptual ambiguities and practical constraints

In many African communities, societal behavioural standards are deeply entrenched and function as normative frameworks. These norms are not only internalised through socialisation but are also actively maintained through the communal acceptance of specific behaviours and the rejection, often with resistance, of foreign practices perceived as externally imposed (Hage 2018). This dynamic can either hinder or facilitate the assimilation of relatively foreign legal and cultural constructs, such as the ‘right to privacy.’ Since communal belonging is historically and culturally embedded within African societies, societal needs and values shifts may influence the underlying instinctual structures that shape behaviour. As Varga (2012) notes, transformations in societal needs can provoke corresponding changes in social conduct. Therefore, for privacy to be meaningfully recognised as a social need within the intricate fabric of African social structures, it is crucial that data protection frameworks do not result in rigid forms of legal regimentation. As Bygrave (2014) warns, privacy must not be framed as an antisocial luxury attainable only through considerable hardship. In contexts where socially constructed needs and aspirations may conflict with perceived notions of privacy, viewed as disruptive to established norms, there is a risk of undermining its legitimacy. Consequently, legal frameworks that address the unique needs of African societies should aim to reinforce their constitutional legitimacy by ensuring that the laws enacted are in harmony with the prevailing societal standards and values upon which lawful authority depends.

Early adopters of privacy legislation in Africa, particularly former French colonies, did so largely in response to directives from their former colonial power (Bygrave 2014). In more recent times, the digitalisation of African economies and the growing imperative for global economic integration have driven several nations to adopt data protection principles more aligned with the lived realities and needs of their populations. Consequently, the shift towards comprehensive data protection frameworks underpinned by legislative acts in countries such as Kenya and Nigeria has enhanced legal effectiveness and strengthened the enforcement capabilities of regulatory authorities. The roles of these data protection agencies, often modelled on global best practices – most notably the General Data Protection Regulation (GDPR) – are reinforced by statutory provisions that increase enforceability. This is crucial, as compliance is significantly dependent on the administrative capacity and reach of a Data Protection Authority (DPA).

Nevertheless, several inherent challenges continue to undermine the ability of these regulatory agencies to fully execute their mandates. While the incorporation of international best practices is essential for legal harmonisation and legitimacy, such principles must be carefully contextualised within the socio-economic conditions specific to each jurisdiction. In the case of Kenya and Nigeria, effective operationalisation of data protection rules requires a nuanced understanding of local enforcement challenges and broader socio-legal realities. Without such contextualisation, there is a risk that these frameworks may remain aspirational in nature, rather than achieving meaningful regulatory impact.

#### 4.1.1. The tension between privacy and national security

The presence of ‘Big Brother’ in the African context is an observable reality, wherein state-run agencies equipped with advanced surveillance technologies actively encroach upon

citizens' personal data (Roberts et al. 2023).<sup>36</sup> Striking an appropriate balance between safeguarding data privacy and addressing national security concerns poses a substantial challenge for effective privacy enforcement (Case C-623/17 para22; Case C-511/18 para58, 65). The Kenyan and Nigerian data protection frameworks permit exemptions from data-related obligations in the interest of national security, law enforcement, and public safety. While such exemptions are arguably necessary for state functionality, they also create potential loopholes through which individual privacy rights may be compromised. In particular, these provisions can legitimise state-sanctioned surveillance and other forms of data misuse by government agencies, thereby weakening the integrity of the broader data protection regime.

Kenya's broad provisions raise concerns about the potential of state surveillance in a political climate grappling with heightened concerns of counterterrorism and national security. The nation's geopolitical positioning, with proximity to Somalia serving as Al-Shabaab's stronghold, coupled with extremist threats, has facilitated an increase in state surveillance measures.<sup>37</sup> As a result, individual data protection is likely to be subordinated to security concerns, whereby transparency or oversight on personal data use by government agencies is limited.<sup>38</sup> Similarly, balancing privacy and security concerns, Nigeria's framework is shaped by a different security dynamic. The threat of insurgencies in the Northeast and widespread concerns about political instability have elevated national security above privacy considerations in its governance framework (Privacy International 2018).<sup>39</sup> The framework's integrity is further strained by a lack of transparency on the use of personal data, with various civil society organisations demanding clarity in the use and raising concerns on the potential for abuse in the context of political dissent and human rights activism.<sup>40</sup>

This tension highlights a core issue in the privacy discourse on assessing the balance of individual rights and the need for collective security. Although explicitly providing safeguards, the lack of transparency around the security exemptions brings the overall integrity of the enforcement framework into question. As Privacy International observed, this covert subversion of privacy under the guise of security in the Global South has largely been driven by a political need, particularly during election cycles, when incumbent governments seek to deliberately restrict opposition figures or activists (Privacy International 2018).<sup>41</sup>

#### **4.1.2. Enforcing rights**

Observing that the trend in privacy legislation was directed towards granting individuals more privacy protection, Posner (1978) argued that an ideal legislative framework should instead accord private businesses more protection. However, the former was adopted mainly by governments, as showcased by two data protection frameworks granting privacy rights to individuals over control of their data, aligning broadly with the rights conferred under the GDPR. However, despite the formal recognition of these rights, the accessibility to exercise the rights remains elusive to the average citizen, particularly in Nigeria, with a larger population. Solove and Schwartz (2021) argue that mere recognition and formalisation of rights under statutory provisions is insufficient. Thus, the need to be supplemented by accessible mechanisms to exercise the rights is core to the operationalisation of a comprehensive data protection framework. Furthermore, practical constraints may be reflected in the lack of specificity in the scope and limits regarding the right to

rectification and erasure. The absence of clear guidance for businesses on the timelines for these provisions substantially weakens the framework risking overbearing and misallocation of resources in pursuit of issues rather well addressed through time-bound obligations.

#### **4.1.3. Consent and legitimate interest**

As in many global privacy regimes, the concept of consent serves as a foundational principle in both Kenya's Data Protection Act (DPA) and Nigeria's Data Protection Act (NDPA), reflecting a rights-based approach to data governance. However, the notion of consent is fraught with conceptual ambiguities, particularly due to data subjects' limited understanding of the implications of consenting to data processing (Solove 2024). This raises critical concerns regarding the effectiveness of informed consent as a legal standard. The challenge is further compounded by the socio-economic realities in both Kenya and Nigeria, where low levels of digital literacy and awareness may lead individuals to prioritise access to essential services over the safeguarding of their personal data. In such contexts, consent risks becoming a perfunctory exercise rather than a meaningful safeguard against data exploitation.

Solove (2024) highlights that, even in the United States, determining whether individuals were explicitly informed about the terms of data processing is central to assessing privacy infringements. The same principle applies in the Global South, where regulatory authorities must take proactive steps to enhance public understanding. This includes mass public education campaigns, the issuance of clear and detailed guidelines on what constitutes informed consent, and the imposition of explicit duties on data controllers and processors. Importantly, legal provisions on consent should move beyond broad and generic language to focus on the clarity and simplicity of communication by processors, ensuring that data subjects fully comprehend the intended purposes of data collection.

Moreover, the potential for high compliance costs to discourage the implementation of such robust consent mechanisms must be acknowledged. It is essential that the development of regulatory guidance takes into account the diversity of data subjects and prioritises resource allocation towards the promotion of best practices, through preventive measures and education, rather than relying solely on remedial action after infringements occur. In doing so, the framework for informed consent can serve as a practical and effective tool in protecting privacy rights, rather than remaining a merely formalistic requirement.

Furthermore, the reliance on legitimate interest as a lawful basis for data processing presents significant challenges, as it may be used to justify intrusive data practices. This concern is particularly evident in sectors such as telecommunications and fintech, where large volumes of personal data are collected and processed daily – enabled by the widespread adoption of mobile technologies. In contrast to the General Data Protection Regulation (GDPR), which subjects legitimate interest claims to rigorous assessments and balancing tests to safeguard data subjects' rights, both the Kenyan DPA and the Nigerian NDPA lack a clearly articulated evaluative framework for determining what qualifies as a legitimate interest.

The absence of such guidance places the burden of interpretation on data controllers and processors, thereby increasing the risk that personal data may be processed in ways

that are not aligned with the principles of necessity and proportionality. This regulatory ambiguity weakens the protective function of data protection laws and may result in inconsistent enforcement and diminished accountability. As such, the development of clear, context-specific criteria and oversight mechanisms is essential to ensure that claims of legitimate interest do not erode individuals' privacy rights.

## ***4.2. Institutional structures and capacity gaps***

### ***4.2.1. Structural and capacity gaps***

In light of the structural and contextual differences underpinning the institutional approaches to privacy, this analysis explores the divergent enforcement landscapes shaped by distinct institutional frameworks and capacity challenges. In the case of Kenya's Office of the Data Protection Commissioner (ODPC), the regulatory approach is anchored in broader principles of trust-building and transparency, underpinned by a commitment to sound governance and effective leadership.<sup>42</sup> Closer examination reveals that the ODPC's strategy prioritises three core areas: regulatory services, encompassing compliance and enforcement, public awareness, and institutional capacity development. Ideally, these focus areas are expected to catalyse change across legal, policy, and institutional frameworks, as well as stimulate research partnerships and collaborative initiatives.<sup>43</sup>

Conversely, Nigeria's Data Protection Commission (NDPC) frames its mandate within a broader vision of developing a resilient digital economy, structured around five strategic pillars: governance, ecosystem and technology, capacity development, cooperation and collaboration, and funding and sustainability.<sup>44</sup> At the implementation level, these pillars reflect the Commission's broader objectives, underscoring an ambitious regulatory agenda. However, the success of this approach hinges on coherent and coordinated execution, particularly in aligning strategic aims with institutional capacity and operational realities.

In considering the strategic roadmaps laid out by the respective data protection authorities, Kenya currently stands just beyond the development of sector-specific toolkits, whereas Nigeria has progressed to the mid or final stages of implementing the NDPA, including the articulation and execution of public awareness campaigns. While the establishment of Kenya's Office of the Data Protection Commissioner (ODPC) marked a significant step in formalising the country's enforcement architecture, its early institutional fragility raised legitimate concerns about its capacity to deliver effective oversight. In particular, limited financial and human resources constrained the ODPC's ability to monitor compliance comprehensively across diverse sectors. In practice, this resource deficit undermined the deterrent effect of the regulatory framework, with some organisations breaching data protection obligations under the assumption that enforcement would be minimal or symbolic.

However, many of these initial limitations have since been addressed, as reflected in the number of high-profile enforcement actions undertaken by the ODPC in 2023. These cases suggest that the agency has begun to establish the foundational institutional strength necessary to assert its regulatory authority across both public and private domains. Furthermore, the ongoing expansion of the ODPC's presence across Kenya – aligned with broader governmental efforts to devolve administrative functions –

represents a significant step toward enhancing its reach and responsiveness.<sup>45</sup> The transition from a centralised national regulator to a more decentralised model with regional offices signals the emergence of a more robust institution capable of swiftly addressing data protection infringements.

Nonetheless, this institutional evolution is resource-intensive, necessitating sustained political commitment to ensure that data protection remains a national priority amid competing policy agendas. This is especially pertinent in light of developments such as the Finance Bill 2024, which underscores the ongoing tension between economic policy imperatives and the need to safeguard fundamental rights.<sup>46</sup> Therefore, political reassurances and budgetary allocations that reflect the strategic importance of data governance are essential to consolidate the ODPC's gains and ensure long-term regulatory efficacy.

Nigeria's enforcement landscape, though relatively young, faces similar challenges to Kenya's ODPC in its formative years. The agency faces resource limitations, particularly in terms of funding and expertise, coupled with the vast and heterogeneous economic sectors, presenting a source of potential enforcement challenges. However, having shifted from a system riddled with regulatory fragility, the concrete implications of enforcement under the NDPA framework offer a deterrent framework which bolsters its investigative and corrective measures. Additionally, uniform application of the NDPA on both informal and multinational corporations will require a flexible but effective enforcement strategy. Ideally, this would take the form of the NDPC prioritising high-impact cases paired with support for capacity building targeted at smaller enterprises, pivotal towards the consolidation of its enforcement powers. Critical to the solidification of its position is the need to have personnel with the capacity to carry out the mandate of the agency. The personnel, coupled with technical tools to facilitate auditing and enforcement, will be able to fulfil the agency's broad enforcement mandate. Theoretically, this facilitates effective governing of data in Nigeria's fast-paced digital economy. Practically, the NDPA provides an enforcement 'apparatus' that hinges on a robust legislative backing to compel compliance; the NDPC's decisive need moving forward will be to balance the framework against competing interests such as national security and economic policy.

#### ***4.2.2. Compliance and monitoring: technical and organisational***

The proliferation of data protection laws has brought about significant challenges for organisations in the need to demonstrate compliance, particularly in the face of dynamic consent. Furthermore, this is complicated by the calls for data protection by design which bring about technical challenges. According to the International Association of Privacy Professionals (IAPP-EY) Privacy Governance Report 2023, about three-fifths of organisations utilise a global privacy compliance programme, varying levels depending on jurisdictions (International Association of Privacy Professionals 2023). Of the surveyed organisations, about 90% are somewhat confident of their organisation's privacy compliance (ibid). These metrics, restricted to 50 countries, are limited to reflect organisational perspectives and devoid of institutional perspectives. Therefore, a comprehensive report on the trends in enforcement, showcasing compliance verification and considering non-compliance with provisions resulting in fines, is lacking. However, an outlook on the challenges of an enforcer assessing compliance will offer insight into approaches to guiding



the implementation of comprehensive processes in the form of technical and organisational measures.

The DPA and NDPA require organisations to adopt technical and organisational measures geared towards securing personal data.<sup>47</sup> Additionally, the DPA has provisions on processing through data centres or servers in Kenya, highlighting the need for global integration. At the core of ensuing compliance are provisions emphasising on breach notifications in the two legislative frameworks, mirroring GDPR provisions.<sup>48</sup> However robust, the efficacy is constrained by a lack of access to resources and a culture of corporate non-compliance. It is further strained by the respective jurisdictions' provisions on data transfer obligations, which are reliant on the determination of adequate safeguards. Although the determination serves to solidify their positions in the global digital economy, in Nigeria, this raises concerns about the capacity of enterprises to comply with data protection standards beyond their national applicable rules within an underdeveloped framework still set on addressing issues on specificity and clarity.

Moreover, in both Kenya and Nigeria, the provisions governing data transfers rely on consent, which, as previously discussed, is not always 'informed' as intended. Although the frameworks appear robust, particularly in addressing data processing through servers located within Kenya, there is a discernible risk stemming from their foundation in strategic interests that echo the Washington Consensus era, primarily economic in nature, which may override the safeguarding of data in the global context (Babb 2013; Begazo et al. 2024).<sup>49</sup> The consequence is the creation of regulatory frameworks that may impose excessive compliance costs on enterprises, increasing the likelihood of many, especially small businesses, resorting to ad hoc data transfer arrangements.

To prevent a rise in data breaches and non-compliance, regulatory agencies should design their compliance regimes to accommodate both high-profile and small to medium-sized enterprises. This includes addressing the distinct needs of smaller entities, which often lack the financial and technical capacity to implement adequate security measures, as well as larger organisations, which, while more resourceful and influential, may pose risks of regulatory capture. A tailored approach would simultaneously reduce the compliance burden on firms and promote their fuller integration into the data protection framework (Ayres and Braithwaite 1992).

#### ***4.2.3. Legitimacy deficit in institutional structure***

Gasser and Schulz (2015) argue that regulatory legitimacy is essential for effective enforcement. In both countries, this perceived legitimacy is strained by the lack of transparency and accountability in the enforcement practices, particularly in the case of the NDPC. Furthermore, the degree of independence and accountability standards is questionable due to the retention of immense influence by the executive arm of the government. This is showcased in the DPA and NDPA, which have broad provisions on the powers of the cabinet secretary or minister in issuing directives for the authorities to comply with.<sup>50</sup> This critical limitation places the regulatory authorities in a precarious position where their regulatory legitimacy is at risk of being reduced to merely a reflection of the administrative directives.

The ODPC operates with a relatively high degree of autonomy from political interference, credited to the provisions granting the office financial independence and legal protection. This autonomy facilitates the agency to carry out its mandate without the

fear of political reprisal when enforcing the law against incumbent corporations or state actors. This is demonstrated in the increasing capacity to engage in high-profile enforcement actions, such as executing data impact assessments on government agencies and the scrutiny of firms processing significant amounts of personal data.<sup>51</sup> Additionally, with an expansive mandate covering all aspects of data processing, compliance monitoring, complaints handling, and the issuance of penalties, the ODPC's strong legal foundation and a higher degree of legitimacy facilitated the decentralisation of powers to constituent offices.

In contrast to the Kenyan model, the NDPC's autonomy is threatened by underfunding and limited technical capacity. The budgetary allocation to the NDPC presents a privacy enforcement framework that is operationalised through funding from other sectoral regulators, unlike in Kenya, where the national assembly directly allocates funding for the authority.<sup>52</sup> The 'agency dependent' budgetary provisions risk exerting influence over the NDPC by the other sectoral regulators, rather than coordination in the regulation of the digital economy, raising concerns on the NDPC's ability to compel compliance. Ideally, the NDPC should ensure there is no overlapping of regulatory interests, which may create business uncertainty, thus reducing the overall effectiveness of privacy enforcement arising from the divergent approaches of the agencies. Perhaps looking into framing an outlook similar to Kenya's ODPC will ensure the enforcement framework benefits from a more structured financing agreement, as within the framework of the DPA.<sup>53</sup>

### **4.3. The socio-economic and political context**

#### **4.3.1. Public awareness and digital literacy**

The transposition of governance frameworks from developed to developing economies must consider the local conditions of the intended destination (Castells 1998; Sassen 2007). Although emulating global best practices in data protection, the two agencies are tasked with the realignment of the underlying objectives in accordance with the specific socio-economic conditions that shape data governance. Moreover, the reliance on market-based compliance mechanisms assumes a level of corporate responsibility that may be lacking in small to medium enterprises. Although considered good practice and key to regulatory resource allocation, the use of self-reporting and data audits may have the adverse effect of straining business resources and widespread non-compliance. This presents a significant enforcement gap in Nigeria since monitoring compliance across the vast number of informal enterprises handling data is compounded by the lack of institutional capacity. Ideally, this would best be addressed through scaling up of both technical and organisational resources, particularly the establishment of regional administrative hubs, as in the case of Kenya.

A common challenge in Kenya and Nigeria is the low level of public awareness regarding data protection rights and obligations. Effective privacy enforcement, particularly in the Global South, is influenced by the public's perception and their assertion of rights as data subjects (Cho, Rivera-Sánchez, and Lim 2009). Although both the DPA and the NDPA grant individuals rights over their personal data, the effectiveness of exercising the rights is largely undermined by the public's lack of knowledge of their existence. In Kenya, the issue stretches beyond the confines of public awareness to stark disparities

in digital literacy, particularly between the rural and urban populations (Okello 2023). While the proliferation of tech-led advancement, compounded with mobile penetration rates, suggests a digitally savvy population, the reality is more nuanced. Whereas cities experiencing the burgeoning of the tech sector are relatively informed, the rural citizens are largely unaware of their data protection rights. Moreover, the marginalised few who are aware often lack the resources or institutional support to exercise their rights effectively.

Beyond geographical situs, digital literacy is also shaped by the socioeconomic status of the citizens (Kerkhoff and Makubuya 2022). Wealthier urban populations are better positioned to access information about data protection and, therefore, are more likely to assert their rights. On the other hand, the marginalised, most vulnerable to data exploitation, are less likely to exercise their rights under the data protection framework. Although more profound than the Kenyan enforcement sphere, the Nigerian context is exacerbated by the larger population and greater digital divide (Ajonbadi, Olawoyin, and Adekoya 2023). Mirroring the rural realities of the Kenyan population, public awareness of the NDPA and digital literacy remains low. As a result, many citizens are unaware of the rights granted under the NDPA framework and thus cannot seek redress for data infringement. The low levels of public engagement can create a passive enforcement environment where violators go unreported and sanction-free, thereby weakening the effectiveness of the privacy protection framework. Furthermore, the risk of creating an 'enforcement framework taxonomy,' where the full benefits of data protection are disproportionately felt by those with the resources to engage with the legal system actively, is best addressed in the implementing stages of structures of enforcement.<sup>54</sup>

Although ultimately ensuring sound enforcement since the authorities shape the enforcement regime to their image, they face the challenge of building up an enforcement regime from where it was non-existent, rather than building upon, which is resource-intensive. Furthermore, individuals are less likely to know of their privacy rights or have the means to lodge complaints, which consolidates the issue of many small and medium enterprises operating at the periphery of enforcement reach. In Nigeria, the issue is severe, arising from a more geographically dispersed population with a significant proportion of the economy operating in the informal sector.

#### **4.3.2. Political interference**

An advantage that the ODPC enjoys is its relative independence from political interference. With a strong legal mandate to act independently of the executive branch, the Commissioner is appointed through a transparent process, including parliamentary oversight. This bolsters the office's powers to pursue enforcement actions across public and private entities. However, there are instances where the independence suffers from political pressures arising from the government's interest in digital economic growth (Begazo et al. 2024).<sup>55</sup> The government's push for deregulation in select sectors to enhance foreign investment has imposed additional responsibilities on the Office of the Data Protection Commissioner (ODPC). Consequently, the ODPC is tasked with navigating the complex interplay between promoting innovation and upholding compliance with data protection legislation – an equilibrium it has, to date, managed to sustain effectively.

In contrast, the NDPC operates in a more politically charged environment, where political interference is a more pressing concern. Although the agency is independent, it

faces the challenges of the government subjecting it to broader policy prioritising economic growth and digital innovation over strict enforcement. This is compounded by the creation of the Council to which the Commissioner is subordinate, whereby the decision-making process relies on the Council's deliberations. Conversely, the Commissioner's powers are meant to be consolidated by the Council, whereby the Commissioner's office is strategically placed as the sole formal decision maker. Furthermore, the strategic direction of the NDPC should be vested on the Commissioner, with the council acting as a collective decision-making management board. Ideally, the council should operate on a majority vote principle on matters where a consensus is elusive, with the Commissioner being capable of making decisions contrary to the Council's view. This decision-making model, in line with good practice, having the commissioner positioned as the chair rather than the secretary, would have the effect of ensuring that the independence of the NDPC is inviolable.

## 5. The way forward

This article delves into the structure and decisions of the DPAs, veering from the role of the courts, and explores the implementation of the legislative framework by the regulators as autonomous enterprises (Mashaw 2005).<sup>56</sup> In light of external influences and the formation of internal norms, the analysis delves into a series of institutional challenges that mirror each other but with different underlying determinants. It further points out that the data protection frameworks under assessment are faced with competing interests with legitimate economic and public interest goals complicating the enforcement of the rules, compounded by the balance between regulatory policy and politics. The paper aligns with Murphy's (2018) argument that, although the pervasive view of the law being in a losing race with technology, legislators should ideally 'future-proof' legislation, which is core to technology regulation.

The foregoing analysis highlights that while Kenya and Nigeria's data protection mechanisms are grounded in emerging legislative frameworks, they diverge in institutional robustness and enforcement rigour. The divergence is multifaceted and shaped by several factors, including institutional autonomy, resource allocation, and socio-political dynamics, all of which have profound implications for the ability of the agencies to protect personal data in an increasingly digital economy. Offering insight into the core of the two regimes, it points out that at the foundation lies a legal framework that provides a statutory basis for institutional independence. As discussed, the ODPC enjoys a relatively higher level of autonomy. In contrast, the NDPC's approach raises concerns of heightened political interference and therefore a need for greater transparency, fostering trust in its regulatory competency.

The discussion further highlights that Kenya's Office of the Data Protection Commissioner (ODPC) benefits from a relatively well-structured and adequately resourced enforcement framework, which enables it to conduct investigations and impose penalties for non-compliance. The substantial number of fines issued to date may be interpreted as serving a deterrent function. Moreover, these penalties contribute significantly to meeting the financial requirements of both the ODPC and the NDPC. While the existing fee structure has been designed with consideration of the country's socio-economic context, the analysis underscores the need for a reassessment, given that current fees

represent a substantial undervaluation. Such a reassessment would not only enhance the agencies' ability to meet their financial obligations but also support the scaling up of their technical and organisational capacities. Additionally, the discussion advocates for the ODPC to adopt a tiered fining structure – similar to that employed by Nigeria – where data handlers are categorised according to their significance (e.g. high or low importance). This would allow for the application of administrative discretion on a case-by-case basis instead of relying on a uniform approach.

Given the persistently low levels of public awareness and digital literacy across the country, particularly within rural and low-income areas where the informal sector continues to expand, the allocation of enforcement resources remains a significant challenge. In this context, both the NDPC and ODPC are entrusted with the critical responsibility of promoting public awareness and fostering compliance. Therefore, these agencies must intensify their outreach through targeted public awareness campaigns, developed in collaboration with local communities. Under the leadership of the Commissioner, the NDPC could consider establishing regional engagement and enforcement hubs, a model already being explored in Kenya as its enforcement mandate becomes more firmly established. Such a framework would play a crucial role in bridging the enforcement gap, ensuring that businesses operating within the informal and rural sectors are brought within the ambit of the data protection regulatory regime.

The analysis further reveals that institutional capacity to enforce compliance remains a significant challenge, particularly in the private sector. Criticism often stems from the perceived disproportionate focus of regulatory agencies on larger, more visible corporations, which may result in underenforcement among smaller or less prominent entities. Both countries, therefore, face an urgent need to strengthen institutional capacity – not only through increased budgetary allocations but also through enhanced collaboration with international partners and civil society organisations. Such efforts would contribute to the development of robust technical and organisational capabilities, thereby ensuring that enforcement mechanisms remain effective in a rapidly evolving digital environment. Moreover, recognising that regulatory coherence is inherently dynamic and must evolve in tandem with technological advancements, Data Protection Authorities (DPAs) should institutionalise regular monitoring and evaluation mechanisms to assess and refine the effectiveness of their enforcement frameworks over time.

Finally, the analysis underscores the critical role of civil society organisations and consumer advocacy groups in promoting data privacy awareness, advocating for robust enforcement, and serving as regulatory watchdogs. In Kenya, the contributions of the Kenya ICT Action Network (KICTANet) have been particularly noteworthy, with sustained engagement with the Office of the Data Protection Commissioner (ODPC) enhancing transparency in enforcement practices and strengthening the protection of data subjects' rights (Varga 2012). Comparable efforts in Nigeria are exemplified by the work of the Paradigm Initiative, which has been at the forefront of digital rights advocacy (Bygrave 2014). Although such initiatives remain relatively limited and the broader landscape of consumer advocacy is still underdeveloped, there is growing public trust in regulatory institutions. This is reflected in the increased public engagement on matters related to data privacy, indicating a positive trajectory toward stronger citizen participation and accountability in data governance.

## 5.1. Conclusion

Based on the comparative analysis, several key recommendations emerge for strengthening privacy enforcement in both Kenya and Nigeria, as well as for other African countries aiming to enhance their data protection regimes. This is particularly crucial as the continent continues its rapid digital transformation, making robust data protection frameworks increasingly indispensable. As two of Africa's leading economies, Kenya and Nigeria are uniquely positioned to set a regional precedent in privacy enforcement. While Kenya has made notable strides, particularly through the operationalisation of the Office of the Data Protection Commissioner (ODPC), Nigeria's data protection framework remains in need of significant reform to improve its overall effectiveness. The experiences and lessons derived from these two jurisdictions can serve as valuable reference points for other African nations seeking to safeguard personal data in an increasingly data-driven global context. Moving forward, it is imperative to prioritise the development of strong, independent regulatory institutions, ensure sufficient resource allocation, and cultivate a culture of compliance across both public and private sectors. Only through addressing these foundational challenges can African countries fully realise the promise of their data protection laws and uphold the rights of individuals in the digital age.

## Notes

1. Angola, Benin, Chad, Congo, Egypt, Gabon, Gambia, Guinea-Bissau, Lesotho, Mauritania, Namibia, Niger, São Tomé and Príncipe, Senegal, and Zambia.
2. UK Government, 'Transforming for a Digital Future: 2022–2025 Roadmap for Digital and Data' (UK Government, updated September 2023) <https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025/transforming-for-a-digital-future-2022-to-2025-roadmap-for-digital-and-data> accessed 24 September 2024.
3. GSMA, The Mobile Economy: Sub-Saharan Africa 2024 (GSMA 2024) [https://event-assets.gsma.com/pdf/GSMA\\_ME\\_SSA\\_2024\\_Web.pdf](https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf).
4. Kenya Information and Communications Act No. 2 Of 1998, s31; Kenya Information and Communications (Consumer Protection) Regulations, 2010.
5. The HIV and Aids Prevention and Control Act Chapter 246A, V.
6. Credit Reference Bureau Regulations, 2013.
7. The Prevention of Terrorism Act Chapter 59B s35(3a); The National Intelligence Service Act, 2012 s36.
8. UNCTAD, Harmonizing Cyberlaws and Regulations: The Experience of the East African Community (UNCTAD 2012) 17 [https://unctad.org/system/files/official-document/dtlstict2012d4\\_en.pdf](https://unctad.org/system/files/official-document/dtlstict2012d4_en.pdf) accessed 24 September 2024.
9. *ibid* 21.
10. Constitution of Kenya, 2010 Art31.
11. DPA s4.
12. DPA s26
13. DPA VII.
14. The Data Protection Act Subsidiary Legislation NO. 24 OF 2019.
15. Nigeria Data Protection Regulation 2019
16. NITDA Act, 2007 s6(a)(c).
17. NITDA, Nigeria Data Protection Regulation Performance Report 2019–2020 9.
18. DPA s49.
19. NDPA s42.
20. DPA s32; NDPA s26.

21. General Data Protection Regulation (EU) 2016/679 of The European Parliament and of The Council Art 4(11) rec32.
22. DPA s19(e); NDPA s29(c).
23. DPA s49; NDPA s42.
24. Office of the Data Protection Commissioner (ODPC), 'Determinations' (ODPC 2024) <https://www.odpc.go.ke/determinations/> accessed 24 September 2024.
25. Nigeria Data Protection Commission, *Annual Report 2023* (NDPC 2023) 6 <https://ndpc.gov.ng/Files/AnnualReport2023.pdf> accessed 24 September 2024.
26. Information Regulator (South Africa), 'Media Statement: Infringement Notice Issued to the Department of Justice and Constitutional Development' 4 July 2023 (Information Regulator 2023) <https://infoeregulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf> accessed 24 September 2024.
27. General Data Protection Regulation (EU) 2016/679 rec8.
28. Dongyeon Kim et al, 'Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services' (2019) <https://doi.org/10.1016/j.chb.2018.11.022> accessed 24 September 2024; Sasha Romanosky & Alessandro Acquisti, 'Privacy Costs and Personal Data Protection: Economic and Legal Perspectives' (2009) 24 Berkeley Tech LJ 1061, 1063; Nir Kshetri, 'Big Data's Role in Expanding Access to Financial Services in China' Volume 36, Issue 3, (June 2016) 297 <https://doi.org/10.1016/j.ijinfomgt.2015.11.014> accessed 24 September 2024.
29. DPA s56(5).
30. GAID Art40(13).
31. George I Balch, 'The Stick, the Carrot, and Other Strategies: A Theoretical Analysis of Governmental Intervention' (1980) 2 *Law & Policy* 35 <https://doi.org/10.1111/j.1467-9930.1980.tb00203.x> accessed 24 September 2024; Hazel Grant and Helen Crowther, 'How Effective Are Fines in Enforcing Privacy?' in David Wright and Paul De Hert (eds), *Enforcing Privacy* (Springer 2016) vol 25, Law, Governance and Technology Series 290 [https://doi.org/10.1007/978-3-319-25047-2\\_13](https://doi.org/10.1007/978-3-319-25047-2_13) accessed 24 September 2024.
32. DPA s63.
33. ODPC, 'ODPC TO Audit 40 Digital Lenders and Issues Enforcement Notice Against a Health Service Provider' (ODPC 2023) <https://www.odpc.go.ke/wp-content/uploads/2024/02/Approved-Press-Release-on-DCP039s-and-Health-Provider-1-1.pdf> accessed 24 September 2024; NDPC 2023 n36 20.
34. ODPC, 'ODPC Consolidated Complaints No. 1843 of 2023 (ODPC 2023) <https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-CONSOLIDATED-COMPLAINTS-NO.1843-OF-2023-1971199120062025-2292-OF-2023-DETERMINATION.pdf> accessed 24 September 2024.
35. NDPC 2023 n36 20.
36. For example, See George Orwell, 1984.
37. Privacy International, *Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya* (Privacy International 2017) [https://privacyinternational.org/sites/default/files/2017-10/track\\_capture\\_final.pdf](https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf) accessed 24 September 2024.
38. Victor Kapiyo, Cherie Oyier, and Francis Monyango, *Surveillance Laws and Technologies Used in Countering Terrorism and Their Potential Impact on Civic Space* (Kenya ICT Action Network (KICTANet), January 2024) <https://www.kictanet.or.ke/reports/> accessed 24 September 2024.
39. Privacy International, *The Right to Privacy in Nigeria: Stakeholder Report for the 31st Session of the UPR* (Privacy International 2018) [https://privacyinternational.org/sites/default/files/2018-05/UPR\\_The%20Right%20to%20Privacy\\_Nigeria.pdf](https://privacyinternational.org/sites/default/files/2018-05/UPR_The%20Right%20to%20Privacy_Nigeria.pdf) accessed 24 September 2024.
40. Institute of Development Studies, *Nigeria Spending Billions of Dollars on Harmful Surveillance of Citizens* (IDS 2023) <https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/> accessed 24 September 2024.
41. Privacy International n60.



42. ODPC, *Strategic Plan 2022/3–2024/5* (ODPC 2021) 24–25 <https://www.odpc.go.ke/wp-content/uploads/2024/03/ODPC-Strategic-Plan.pdf> accessed 24 September 2024.
43. Ibid.
44. NDPC, *Strategic Roadmap and Action Plan (SRAP) 2023–2027* (NDPC 2023) <https://ndpc.gov.ng/Srap.pdf> accessed 24 September 2024.
45. ODPC, 'CS Eliud Owalo Launches the Office of the Data Protection Commissioner's First Regional Office in Mombasa' (ODPC 2023) <https://www.odpc.go.ke/wp-content/uploads/2024/02/CS-Eliud-Owalo-Launches-the-Office-of-the-Data-Protection-Commissioners-First-Regional-Office-in-Mombasa.pdf> accessed 24 September 2024; ODPC, 'PS Eng. John Tanui MBS Launches the Office of the Data Protection Commissioner's Second Regional Office in Nakuru' (ODPC 2023) <https://www.odpc.go.ke/wp-content/uploads/2024/02/PS-Eng.-John-Tanui-MBS-Launches-the-Office-of-the-Data-Protection-Commissioners-Second-Regional-Office-in-Nakuru.pdf> accessed 24 September 2024; ODPC Strategic Plan 31
46. The Finance Bill, 2024 599.
47. DPA s29; NDPA s24(2).
48. DPA 44; NDPA s40; GDPR art33.
49. DPA s72; NDPA s60.
50. DPA s72; NDPA s60.
51. ODPC, 'Press Statement on IEBC Verification of Voting Particulars Portal' (ODPC 2022) <https://www.odpc.go.ke/wp-content/uploads/2024/02/PRESS-STATEMENT-ON-IEBC-VERIFICATION-OF-VOTING-PARTICULARS-PORTAL.pdf> accessed 24 September 2024.
52. NDPA s19(2).
53. DPA s68.
54. see enforcement pyramid in n73.
55. Tania Begazo et al, *Regulating the Digital Economy in Africa: Managing Old and New Risks to Economic Governance for Inclusive Opportunities* (World Bank, 2023) 7 <https://documents1.worldbank.org/curated/en/099051924165027814/pdf/P1724171bc956a07d1bfd6105b3a20f7fa8.pdf> accessed 24 September 2024.
56. Jerry L. Mashaw, 'Between Facts and Norms: Agency Statutory Interpretation as an Autonomous Enterprise' (2005) 55 *University of Toronto Law Journal* 497, 500.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## ORCID

Bukola Faturoti  <http://orcid.org/0000-0001-7610-7910>

## References

- African Union. 2014. *African Union Convention on Cyber Security and Personal Data Protection*. Malabo: African Union. Accessed November 24, 2024. <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.
- Agência de Protecção de Dados. 2024. *APD Multa Africell em 150 Mil Dólares Norte Americanos por Violação da Lei de Protecção de Dados Pessoais (LPDP)*. Luanda: APD. Accessed January 5, 2024. <https://www.apd.ao/ao/noticias/apd-multa-africell-em-150-mil-dolares-norte-americanos-por-violacao-da-lei-de-proteccao-de-dados-pessoais-lpdp/>.
- Ajonbadi, H. A., F. S. Olawoyin, and O. D. Adekoya. 2023. "The Anathema of Digital Divide in the Nigerian Higher Education: Lessons from the Pandemic." In *Beyond the Pandemic Pedagogy of Managerialism*, edited by B. S. Nayak and K. Appleford, 189–208. Cham: Palgrave Macmillan. [https://doi.org/10.1007/978-3-031-40194-7\\_10](https://doi.org/10.1007/978-3-031-40194-7_10).

- Ayres, I., and J. Braithwaite. 1992. *Responsive Regulation: Transcending the Deregulation Debate*. New York: Oxford University Press.
- Babalola, Olumide. 2022. "Nigeria's Data Protection Legal and Institutional Model: An Overview." *International Data Privacy Law* 12 (1): 44–52. Accessed September 21, 2024. <https://doi.org/10.1093/idpl/ipab023>.
- Babb, S. 2013. "The Washington Consensus as Transnational Policy Paradigm: Its Origins, Trajectory and Likely Successor." *Review of International Political Economy* 20 (2): 268–297. <https://doi.org/10.1080/09692290.2011.640435>.
- Balch, George I. 1980. "The Stick, the Carrot, and Other Strategies: A Theoretical Analysis of Governmental Intervention." *Law & Policy* 2 (1): 35–60. <https://doi.org/10.1111/j.1467-9930.1980.tb00203.x>.
- Baldwin, Robert. 1995. "Making Rules Work." *Rules And Government* (Oxford; online edn, Oxford Academic, 31 Oct. 2023). Accessed April 10, 2025. <https://doi.org/10.1093/oso/9780198259091.003.0006>.
- Begazo, T., C. Stinshoff, H. Niesten, G. Pop, R. Chen, and G. Coelho. 2024. "Regulating the Digital Economy in Africa: Managing Old and New Risks to Economic Governance for Inclusive Opportunities." World Bank Publications - Reports 41620, The World Bank Group. <https://documents1.worldbank.org/curated/en/099051924165027814/pdf/P1724171bc956a07d1bfd6105b3a20f7fa8.pdf>.
- Braithwaite, J. 2011. "The Essence of Responsive Regulation." *University of British Columbia Law Review* 44:475.
- Bygrave, Lee Andrew. 2014. "Data Privacy Law: An International Perspective." (Oxford; online edn, Oxford Academic, 16 Apr. 2014). Accessed April 16, 2025. <https://doi.org/10.1093/acprof:oso/9780199675555.001.0001>.
- Case C-511/18 La Quadrature du Net and Others v Premier Ministre and Others [2020] ECLI:EU:C:2020:791.
- Case C-623/17 Privacy International v Secretary of State for Foreign and Commonwealth Affairs [2020] ECLI:EU:C:2020:790.
- Castells, M. 1998. *End of Millennium Vol. 3 of The Information Age: Economy, Society, and Culture*. Oxford: Blackwell.
- Central Bank of Kenya. 2013. *Credit Reference Bureau Regulations*. Nairobi: Government Printer.
- Cho, H., M. Rivera-Sánchez, and Sun Sun Lim. 2009. "A Multinational Study on Online Privacy: Global Concerns and Local Responses." *New Media & Society* 11 (3): 395–416. <https://doi.org/10.1177/1461444808101618>.
- Curtiss, Tiffany. 2018. "Privacy Harmonization and the Developing World: The Impact of the EU's General Data Protection Regulation on Developing Economies." *Washington Journal of Law, Technology & Arts* 13:143. Accessed September 14, 2024. <https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=1268&context=wjlta>.
- Data Protection Act No. 24 of 2019 (Kenya)
- Gasser, U., and W. Schulz. 2015. "Governance of Online Intermediaries: Observations from a Series of National Case Studies." *Korea University law review* 18: 11. [https://dash.harvard.edu/bitstream/handle/1/16140636/Berkman\\_2015-5\\_final.pdf?sequence=1&isAllowed=y](https://dash.harvard.edu/bitstream/handle/1/16140636/Berkman_2015-5_final.pdf?sequence=1&isAllowed=y).
- General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council.
- Grant, H., and H. Crowther. 2016. "How Effective Are Fines in Enforcing Privacy?" In *Enforcing Privacy. Law, Governance and Technology Series()*, edited by D. Wright and P. De Hert, Vol. 25, 287–305. Cham: Springer. [https://doi.org/10.1007/978-3-319-25047-2\\_13](https://doi.org/10.1007/978-3-319-25047-2_13).
- GSMA. 2024. *The Mobile Economy*. London: GSMA. Accessed October 4, 2024. <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf>.
- Hage, J. 2018. "Of Norms." In *Handbook of Legal Reasoning and Argumentation*, edited by G. Bongiovanni, G. Postema, A. Rotolo, G. Sartor, C. Valentini, and D. Walton. Dordrecht: Springer. [https://doi.org/10.1007/978-90-481-9452-0\\_5](https://doi.org/10.1007/978-90-481-9452-0_5).

- IAPP. 2023. "International Association of Privacy Professionals (IAPP-EY) Privacy Governance Report 2023." (IAPP). Accessed September 24, 2024. <https://iapp.org/resources/article/privacy-governance-full-report/>.
- IDS (Institute of Development Studies). 2023. "Nigeria Spending Billions of Dollars on Harmful Surveillance of Citizens." Accessed September 2, 2024. <https://www.ids.ac.uk/press-releases/nigeria-spending-billions-of-dollars-on-harmful-surveillance-of-citizens/>.
- Information Regulator (South Africa). 2023 July 4 "Media Statement: Infringement Notice Issued to the Department of Justice and Constitutional Development." 2023 (Information Regulator). Accessed July 12, 2024. <https://infoeregulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf>.
- Jordana, J., David Levi-Faur, and X. Fernández-i-Marín. 2011. "The Global Diffusion of Regulatory Agencies: Channels of Transfer and Stages of Diffusion." *Comparative Political Studies* 44 (10): 1343. Accessed October 18, 2024. <https://doi.org/10.1177/0010414011407466>.
- Kapiyo, V., C. Oyeir, and F. Moyango. January 2024. *Surveillance Laws and Technologies Used in Countering Terrorism and Their Potential Impact on Civic Space*. Nairobi: Kenya ICT Action Network (KICTANet). Accessed September 2, 2024. <https://www.kictanet.or.ke/reports/>.
- Kenya Information and Communications (Consumer Protection) Regulations, 2010.
- Kenya Information and Communications Act No. 2 Of 1998
- Kerkhoff, Shea N., and T. Makubuya. 2022. "Professional Development on Digital Literacy and Transformative Teaching in a Low-Income Country: A Case Study of Rural Kenya." *Reading Research Quarterly* 57 (1): 287–305. Accessed October 28, 2024. <https://doi.org/10.1002/rrq.392>.
- Kim, D., K. Park, Y. Park, and J. Ahn. 2019. "Willingness to Provide Personal Information: Perspective of Privacy Calculus in IoT Services." *Computers in Human Behavior* 92:273–281. <https://doi.org/10.1016/j.chb.2018.11.022>.
- Kosti, N., D. Levi-Faur, and G. Mor. 2019. "Legislation and Regulation: Three Analytical Distinctions." *The Theory and Practice of Legislation* 7 (3): 169–178. <https://doi.org/10.1080/20508840.2019.1736369>.
- Kshetri, N. 2016. "Big Data's Role in Expanding Access to Financial Services in China." *International Journal of Information Management* 36 (3): 297–308. Accessed January 6, 2024. <https://doi.org/10.1016/j.ijinfomgt.2015.11.014>.
- Mashaw, J. L. 2005. "Between Facts and Norms: Agency Statutory Interpretation as an Autonomous Enterprise." *University of Toronto Law Journal* 55 (3): 497–533. <https://doi.org/10.1353/tlj.2005.0019>.
- Murphy, M. H. 2018. *Surveillance and the Law: Language, Power and Privacy*. 1st ed. London: Routledge. <https://doi.org/10.4324/9780429485466>.
- NDPA (Nigeria Data Protection Act). 2023.
- NDPC (Nigeria Data Protection Commission). 2023. Annual Report 2023. 6. Accessed September 24, 2024. <https://ndpc.gov.ng/Files/AnnualReport2023.pdf>.
- NDPC (Nigeria Data Protection Commission). 2023. Strategic Roadmap and Action Plan (SRAP) 2023–2027. Accessed September 24, 2024. <https://ndpc.gov.ng/Srap.pdf>.
- Nigeria Data Protection Regulation. 2019.
- NITDA (National Information Technology Development Agency Act). 2007.
- NITDA (National Information Technology Development Agency). n.d. Nigeria Data Protection Regulation Performance Report 2019–2020.
- ODPC (Office of the Data Protection Commissioner). 2021. Strategic Plan 2022/3–2024/5. 24–25. Accessed September 24, 2024. <https://www.odpc.go.ke/wp-content/uploads/2024/03/ODPC-Strategic-Plan.pdf>.
- ODPC (Office of the Data Protection Commissioner). 2022. *Press Statement on IEBC Verification of Voting Particulars Portal*. Nairobi: ODPC. Accessed September 24, 2024. <https://www.odpc.go.ke/wp-content/uploads/2024/02/PRESS-STATEMENT-ON-IEBC-VERIFICATION-OF-VOTING-PARTICULARS-PORTAL.pdf>.
- ODPC (Office of the Data Protection Commissioner). 2024. "Determinations." ODPC. Accessed September 24, 2024. <https://www.odpc.go.ke/determinations/>.

- ODPC (Office of the Data Protection Commissioner) Kenya. 2023. "ODPC TO Audit 40 Digital Lenders and Issues Enforcement Notice Against a Health Service Provider." Accessed September 24, 2024. <https://www.odpc.go.ke/wp-content/uploads/2024/02/Approved-Press-Release-on-DCP039s-and-Health-Provider-1-1.pdf>.
- ODPC (Office of the Data Protection Commissioner) Kenya. 2023. "ODPC Consolidated Complaints No. 1843 of 2023." Accessed September 24, 2024. <https://www.odpc.go.ke/wp-content/uploads/2024/02/ODPC-CONSOLIDATED-COMPLAINTS-NO.1843-OF-2023-1971199120062025-2292-OF-2023-DETERMINATION.pdf>.
- ODPC (Office of the Data Protection Commissioner) Kenya. 2023. *CS Eliud Owalo Launches the Office of the Data Protection Commissioner's First Regional Office in Mombasa*. Nairobi: ODPC. Accessed September 24, 2024. <https://www.odpc.go.ke/wp-content/uploads/2024/02/CS-Eliud-Owalo-Launches-the-Office-of-the-Data-Protection-Commissioners-First-Regional-Office-in-Mombasa.pdf>.
- ODPC (Office of the Data Protection Commissioner) Kenya. 2023. *PS Eng. John Tanui MBS Launches the Office of the Data Protection Commissioner's Second Regional Office in Nakuru*. Nairobi: ODPC. Accessed September 24, 2024. <https://www.odpc.go.ke/wp-content/uploads/2024/02/PS-Eng.-John-Tanui-MBS-Launches-the-Office-of-the-Data-Protection-Commissioners-Second-Regional-Office-in-Nakuru.pdf>.
- Okello, F. 2023. *Bridging Kenya's Digital Divide: Context, Barriers and Strategies*. Waterloo: CIGI. DPH-Paper-Okello.pdf (cigionline.org). Accessed September 24, 2024.
- Posner, R. A. 1978. "The Right of Privacy." *Sibley Lecture Series* 22: 404.
- Privacy International. 2017. *Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya*. London: Privacy International. Accessed December 20, 2024. [https://privacyinternational.org/sites/default/files/2017-10/track\\_capture\\_final.pdf](https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf).
- Privacy International. 2018. *The Right to Privacy in Nigeria: Stakeholder Report for the 31st Session of the UPR*. London: Privacy International. Accessed September 24, 2024. [https://privacyinternational.org/sites/default/files/2018-05/UPR\\_The%20Right%20to%20Privacy\\_Nigeria.pdf](https://privacyinternational.org/sites/default/files/2018-05/UPR_The%20Right%20to%20Privacy_Nigeria.pdf).
- Quach, S., P. Thaichon, K. D. Martin, et al. 2022. "Digital Technologies: Tensions in Privacy and Data." *Journal of the Academy of Marketing Science* 50 (6): 1299–1323. <https://doi.org/10.1007/s11747-022-00845-y>.
- Radovanović, D., C. Holst, S. Belur, R. Srivastava, G. Hounghonon, E. Le Quentrec, J. Miliza, A. Winkler, and J. Noll. 2020. "Digital Literacy Key Performance Indicators for Sustainable Development." *Social Inclusion* 8 (2): 151–167. <https://doi.org/10.17645/si.v8i2.2587>.
- Republic of Kenya. 2010. *The Constitution of Kenya*. Nairobi: Government Printer.
- Republic of Kenya. 2012. *The National Intelligence Service Act*. Nairobi: Government Printer.
- Republic of Kenya. 2012. *The Prevention of Terrorism Act, Cap. 59B*. Nairobi: Government Printer.
- Republic of Kenya. 2024. *The Finance Bill*. Nairobi: Government Printer.
- Roberts, T., J. Gitahi, P. Allam, L. Oboh, O. Oladapo, Gifty Appiah-Adjei, Amira Galal, et al. 2023. "Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi, and Zambia." The Institute of Development Studies and Partner Organisations. Online resource. <https://hdl.handle.net/20.500.12413/18120>
- Romanosky, Sasha, and Alessandro Acquisti. 2009. "Privacy Costs and Personal Data Protection: Economic and Legal Perspectives." *Berkeley Technology Law Journal* 24 (3): 1061. <https://ssrn.com/abstract=1522605>.
- Salami, E. 2020. "Fingerprint Generated Data: An Evaluation of the Efficacy of the Nigerian Data Protection Regulation." *Computer and Telecommunications Law Review* 26 (7): 184–191.
- Sassen, S. 2007. *A Sociology of Globalization (Contemporary Societies*. 1st edn. New York: W.W. Norton & Company.
- Solove, Daniel J. 2024. "Murky Consent: An Approach to the Fictions of Consent in Privacy Law." *Boston University Law Review* 104:593.
- Solove, Daniel J., and Paul M Schwartz. 2021. *Information Privacy Law*. 7th ed. Boston: Wolters Kluwer.
- The Data Protection Act Subsidiary Legislation No. 24 of 2019. – Kenya

The HIV and Aids Prevention and Control Act Chapter 246A – Kenya

UK Government. updated September 2023. *Transforming for a Digital Future: 2022 to 2025 Roadmap for Digital and Data*. London: UK Government. Accessed September 24, 2024. <https://www.gov.uk/government/publications/roadmap-for-digital-and-data-2022-to-2025/transforming-for-a-digital-future-2022-to-2025-roadmap-for-digital-and-data>.

UNCTAD (United Nations Conference on Trade and Development). 2012. *Harmonizing Cyberlaws and Regulations: The Experience of the East African Community*. Geneva: UNCTAD. 17. Accessed September 24, 2024. [https://unctad.org/system/files/official-document/dtlstict2012d4\\_en.pdf](https://unctad.org/system/files/official-document/dtlstict2012d4_en.pdf).

Varga, C. 2012. "Theory of Law: Norm, Logic, System, Doctrine & Technique in Legal Processes, with Appendix on European Law 12 (Szent István Társulat).".

Warren, S. D., and L. D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review*, 4 (5): 193–220. <https://doi.org/10.2307/1321160>