

Bridging the Legal-technical Gap: AI Surveillance and Data Sovereignty in Africa

M Lungu*

Online ISSN
1727-3781

P·E·R

Pioneer in peer-reviewed,
open access online law publications

Author

Maria Lungu

Affiliation

University of Virginia Digital
Technology for Democracy Lab,
Virginia, USA
Kennesaw State University,
Georgia, USA

Email

xta8ym@virginia.edu

Date Submitted

8 September 2025

Date Revised

27 May 2026

Date Accepted

27 May 2026

Date Published

21 July 2026

Guest Editors

Prof Chijioke Okorie
Prof Vukosi Marivate

Journal Editor

Prof Wian Erlank

How to cite this contribution

Lungu M "Bridging the Legal-
technical Gap: AI Surveillance and
Data Sovereignty in Africa" *PER /
PELJ* 2026(29) - DOI
[https://dx.doi.org/10.17159/1727-
3781/2026/v29i0a23860](https://dx.doi.org/10.17159/1727-3781/2026/v29i0a23860)

Copyright



DOI

[https://dx.doi.org/10.17159/1727-
3781/2026/v29i0a23860](https://dx.doi.org/10.17159/1727-3781/2026/v29i0a23860)

Abstract

South African and Nigerian law guarantees rights to privacy and due process, but national security carve-outs and proprietary artificial intelligence (AI) systems shielded from regulatory scrutiny can make those protections difficult to enforce. As African governments progressively rely on foreign vendors for AI-enabled surveillance technologies, a central question is how constitutional protections can be meaningfully enforced when the systems governing surveillance remain technically and legally inaccessible to domestic oversight. The theoretical contribution is the concept of the algorithmic sovereignty gap, which names the persistent disjunction between constitutional guarantees and the operational realities of vendor-controlled tools. Drawing on qualitative content analysis of constitutional law, statutes, case law, and investigative reporting in both countries, and extending Pasquale's black-box problem and Couldry and Mejas's data colonialism framework through a postcolonial lens, the article shows how procurement-led deployment and security exceptions hollow out constitutional rights that the legal texts appear to guarantee. The prescriptive contribution is a hybrid governance model that closes this gap by anchoring transparency and accountability in constitutional baselines, supported by mandatory AI impact assessments, audit rights, source-code escrow, data localisation, and procurement transparency.

Keywords

Surveillance; governance; sovereignty; opacity; postcolonialism; authoritarianism.

.....

1 Introduction

Governments across Africa have adopted AI-powered surveillance¹ technologies to support national security and public order. Facial recognition, IMSI (International Mobile Subscriber Identity) catchers, spyware, biometric identification systems, predictive analytics, or automated data-matching tools,² are procured through public–private partnerships with foreign vendors and promoted based on efficiency gains.³ Constitutional and statutory protections exist, but the regulatory landscape is fragmented, and a gap exists between formal legal rights and surveillance practice.

The gap between formal legal protections and operational surveillance practice is not a regulatory delay that will close as legislation catches up. It is structural. A 2023 Institute of Development Studies study of five African countries (Nigeria, Ghana, Morocco, Malawi and Zambia) found that those governments collectively spent over US\$1 billion per year on digital surveillance technologies, supplied by vendors in the United States (US), the United Kingdom, China, the European Union and Israel.⁴ The study explicitly notes that it covers roughly 10% of African states. Total continental spending is therefore substantially higher. Africa's AI-integrated surveillance market is projected to grow from \$160 million in 2023 to \$772 million by 2030.⁵ Governments justify increased surveillance as a matter of national security or crime prevention.⁶ Still, the pace and scale of investment suggest

* Maria Lungu. JD, PhD. Postdoctoral Research Associate at the University of Virginia Digital Technology for Democracy Lab, Virginia, USA. Dr Lungu is also an Assistant Professor at Kennesaw State University, Georgia. E-mail: xta8ym@virginia.edu or mclungu13@gmail.com. ORCID: <https://orcid.org/0000-0003-0331-8658>.

A version of this article was presented at the *Legal-Technical Governance of AI in Africa Symposium* hosted by the Data Science Law Lab. Thank you to the Data Science Law Lab symposium participants for their valuable feedback, as well as the reviewers and editors of the *Potchefstroom Electronic Law Journal*. This work forms part of the Legal-Technical AI Governance in Africa project hosted by the Data Science Law Lab at the University of Pretoria. The work was supported in part by funding provided to the University of Pretoria through a gift from Meta. The views and opinions expressed in this publication are those of the author(s) and do not necessarily reflect those of the University of Pretoria, Meta, or affiliated institutions.

¹ According to Garner *Black's Law Dictionary*, surveillance is "close observation or listening of a person or place in the hope of gathering evidence". In modern contexts, this includes collecting, analysing and storing personal data, both digitally and physically.

² Lungu "Enhancing Public Service Delivery" 188-204.

³ Taylor 2002 *Surveillance & Society* 66-85; Nandy 2023 *Journal of Current Social and Political Issues* 13-17.

⁴ Roberts *et al Mapping the Supply of Surveillance Technologies to Africa*.

⁵ Haritwal 2025 <https://www.nextmsc.com/report/africa-ai-cctv-market>.

⁶ Chesterman 2021 *AJCL* 271-294.

that AI surveillance is being treated as a normal and expanding function of state power.⁷

Regulation has not kept pace with the deployment of AI technology.⁸ Herein lies a legal-technical gap, reflecting slow legislative progress and a mismatch between law and technological realities.⁹ Joneidy, Rahimian and Arciszewski contend that bridging this divide requires a transdisciplinary strategy that combines technical knowledge with administrative and constitutional principles.¹⁰

Existing scholarship has considered what that transdisciplinary research could look like, and this has been theorised through topics like digital authoritarianism,¹¹ surveillance capitalism¹² and algorithmic harm¹³ primarily situated in the Global North. African legal scholars have also examined data protection¹⁴ and state control of digital infrastructure,¹⁵ but there is limited analysis of how statutory design and implementation address the technical properties and risks of AI systems.¹⁶

This gap matters most when oversight institutions are expected to regulate surveillance systems that they cannot independently examine or fully understand. Therefore, this article asks how constitutional protections for privacy and due process can be meaningfully enforced when AI surveillance systems remain technically opaque and legally insulated from domestic oversight.

This article argues that governance failure stems from three interconnected dynamics. First, algorithmic opacity limits meaningful scrutiny of some internationally procured AI systems and datasets. Second, dependence on foreign vendors creates informational and technical asymmetries between African regulators and the companies supplying surveillance technologies that cannot be independently audited. Third, weak domestic oversight allows broad national security exemptions and limited regulatory authority to become embedded features of the governance system itself. Using qualitative content analysis of constitutional provisions, statutes, regulations, case law and investigative reporting in South Africa and Nigeria, the article examines how these dynamics operate in practice.

⁷ Cayford, Pieters and Van Gelder 2019 *Journal of Information, Communication and Ethics in Society* 10-27.

⁸ Martínez-Béjar and Brändle 2018 *Technology in Society* 139-148.

⁹ Monahan 2008 *Surveillance & Society* 217-226.

¹⁰ Joneidy, Rahimian and Arciszewski 2024 *Law and Business* 1-15.

¹¹ Feldstein *Rise of Digital Repression* 1-20.

¹² Zuboff *Age of Surveillance Capitalism*.

¹³ Eubanks *Automating Inequality*.

¹⁴ Daigle 2021 *Journal of International Commerce and Economics* 1.

¹⁵ Nyabola "Africa's Digital Public Sphere" 315-329.

¹⁶ Roberts *et al* 2021 <https://www.ids.ac.uk/projects/surveillance-legislation-in-africa/>.

A counterinterpretation should be addressed at the outset. The pattern observed in South Africa and Nigeria could reflect a global tendency for constitutional rights to be insufficient against security-driven surveillance, rather than a postcolonial-specific dynamic. The US, where constitutional protections coexist with mass surveillance programs, suggests as much. This article does not claim that postcolonial conditions are the sole cause of the algorithmic sovereignty gap. It argues that postcolonial conditions intensify the gap by adding vendor asymmetry to weak oversight, producing a pattern that Northern frameworks alone cannot fully describe. The two cases are diagnostic, not exhaustive, evidence for this claim.

The argument makes two contributions. The theoretical contribution is the concept of the algorithmic sovereignty gap, which names the persistent disjunction between constitutional guarantees and the operational realities of vendor-controlled tools. The concept is developed by extending Pasquale's black box problem¹⁷ and Couldry and Mejias's data colonialism framework¹⁸ through a postcolonial lens, showing how opacity and data extraction intersect with vendor dependence in ways the original frameworks, developed primarily in the Global North, do not fully address.¹⁹ Other frameworks, such as surveillance capitalism (Zuboff) and digital authoritarianism (Feldstein), inform the analysis but are not central to it.²⁰

Second, the prescriptive contribution is a hybrid governance model that closes this gap by anchoring transparency and accountability in constitutional baselines, supported by mandatory AI impact assessments, audit rights, source-code escrow, data localisation, and procurement transparency.

The article proceeds as follows. Part 2 reviews the relevant literature on AI surveillance frameworks and the theoretical lenses that guide the analysis. Part 3 outlines the case selection and analytic procedure. Part 4 presents findings from both jurisdictions. Part 5 identifies cross-cutting legal-technical challenges. Part 6 proposes the hybrid governance model and the institutional reforms it requires.

¹⁷ Pasquale *Black Box Society*.

¹⁸ Couldry and Mejias 2019 *Internet Policy Review* 1-20.

¹⁹ Couldry and Mejias 2019 *Internet Policy Review* (conceptualise data colonialism as extracting human life for capitalist data production, mirroring historical forms of colonial exploitation).

²⁰ Joneidy, Rahimian and Arciszewski 2024 *Law and Business* 1-15.

2 Literature review and theoretical frameworks

2.1 African surveillance frameworks across the continent

Surveillance technologies have been incorporated into national security and public safety policies across Africa.²¹ Between 2015 and 2024, at least 20 African states enacted or amended laws that authorised governments to intercept communications, evade mandatory data retention requirements, or gain access to subscriber data. In countries like Egypt, Rwanda and Nigeria, these legal instruments often rely on broad, indeterminate references to threats to national interest or public morality, granting executive agencies wide discretion and weakening constraints on surveillance practices.²²

Supporters of digital surveillance and identification systems emphasise their developmental and inclusionary potential.²³ The Rwandan biometric national ID system, covering over 98% of adults, is cited by the World Bank as a best-practice model.²⁴ Such developmental framings often coexist with unaddressed governance risks. The same systems that improve welfare targeting also expand state visibility over citizens, and the literature is divided on whether the developmental gains justify the surveillance expansion they enable.²⁵

However, these ambitions are undermined by significant governance and implementation risks. Civil society actors, including Privacy International, Access Now and the Institute of Development Studies, warn that poorly regulated systems could become "surveillance infrastructures" rather than empowerment tools.²⁶ Data breaches in Nigeria highlight persistent vulnerabilities.²⁷ Moreover, inadequate data protection and cybersecurity laws, often enacted after biometric enrolment begins, expose personal

²¹ Roberts *et al* 2021 <https://www.ids.ac.uk/projects/surveillance-legislation-in-africa/>.

²² Egyptian *Telecommunications Regulation Law* No 10 of 2003; Egyptian *Penal Code* No 58 of 1937; *Constitution of Rwanda*, 2003, art 38; Nigerian *Lawful Interception of Communications Regulations*, 2019.

²³ Sule, Zennaro and Thomas 2021 *Technology in Society* 67.

²⁴ World Bank 2021 <https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0>.

²⁵ World Bank 2021 <https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0>. (Digital IDs also hold the potential to facilitate secure intra-African trade and labour mobility by providing verifiable identity credentials).

²⁶ Privacy International 2023 <https://privacyinternational.org/examples/5291/report-finds-african-countries-adopt-digital-surveillance-despite-human-rights-threat>; Access Now 2024 <https://www.accessnow.org/surveillance/>.

²⁷ INTERPOL 2025 <https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa>.

data.²⁸ Public trust is still tenuous due to this breakdown.²⁹ Further, informed consent is sometimes inconsistent, and many enrollees do not have an accurate or complete understanding of how their data will be used or shared.

At the same time, regulation remains incomplete and uneven. The International Telecommunication Union reports that only about 60% of African states have enacted data protection or privacy legislation.³⁰ The African Union (AU) has called for stronger frameworks to safeguard privacy while ensuring that digital ID systems support economic participation and uphold civil liberties.³¹ The AU's Data Policy Framework promotes data systems that support an inclusive digital economy while protecting rights.³² Achieving this balance requires collaboration between governments and civil society to ensure secure systems.

Regional instruments establish normative benchmarks of legality, necessity, proportionality, and oversight. Principle 40 of the *African Declaration on Freedom of Expression and Access to Information*³³ and Article 9 of the *African Charter on Human and Peoples' Rights*³⁴ require that any interference with privacy be justifiable in a democratic society. The *Malabo Convention*³⁵ extends this framework to data processing. As of August 2025, only fourteen AU member states have ratified the *Malabo Convention*, limiting its regional force. These instruments serve as yardsticks for later evaluation of South African and Nigerian surveillance practices, but domestic implementation frequently omits the proportionality and oversight standards they require.

Despite these commitments, domestic surveillance practices sometimes contradict binding regional and international obligations. The African Commission on Human and Peoples' Rights (ACHPR) Resolution 362 (2016) affirms that the same rights protected offline must also be protected online, including the rights to privacy and freedom of expression.³⁶ Similarly,

²⁸ INTERPOL 2025 <https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa>.

²⁹ Roberts 2025 <https://www.ids.ac.uk/publications/understanding-digital-rights-definitions-conceptions-and-myths/>.

³⁰ UNCTAD 2024 <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>.

³¹ AU 2022 <https://au.int/en/documents/20220728/au-data-policy-framework>.

³² AU 2022 <https://au.int/en/documents/20220728/au-data-policy-framework>.

³³ Principle 40 of the ACHPR *Declaration of Principles on Freedom of Expression and Access to Information in Africa* (2019) (the *Declaration*).

³⁴ Article 9 of the *African Charter on Human and Peoples' Rights* (1981) (the *African Charter*).

³⁵ AU *Convention on Cyber Security and Personal Data Protection* (2014) (*Malabo Convention*).

³⁶ ACHPR *Resolution on the Right to Freedom of Expression and Access to Information on the Internet in Africa* AU Doc ACHPR/Res362(LIX) (2016).

Article 9 of the *African Charter on Human and Peoples' Rights*, and Article 19 of the *International Covenant on Civil and Political Rights (ICCPR)*, guarantee the right to receive and impart information, regardless of frontiers, through any medium.³⁷ The AU's *Declaration of Principles on Freedom of Expression and Access to Information* requires that any surveillance measure be proportionate and subject to oversight.³⁸ However, most of the aforementioned laws omit such standards or provide only nominal compliance mechanisms.³⁹

Domestic enforcement is only one half of the problem. The other half lies in how surveillance capacity reaches African states. Foreign technology partnerships further complicate this regulatory landscape.⁴⁰ AI-powered tools are increasingly part of the national security infrastructure.⁴¹ Reports across jurisdictions suggest that such technologies have been used to monitor opposition actors, journalists and civil society groups, raising additional concerns around data sovereignty and extraterritorial surveillance norms.⁴² These systems are supplied through opaque contracts with foreign firms.⁴³ The opaque nature of these arrangements raises questions about procurement accountability, cross-border data flows and the extraterritorial application of surveillance norms. This evidence lays the groundwork for the article's later argument about vendor dependence and its constitutional implications.

As of 2025, only a handful of African countries such as Kenya (*Data Protection Act* in 2019), Nigeria (*Nigeria Data Protection Regulation* in 2019) and South Africa (*Protection of Personal Information Act* in 2020) have enacted comprehensive data protection legislation. Even where such laws exist, exceptions for "national security" or "public interest" remain undefined, and oversight institutions lack the independence or capacity to monitor AI-driven surveillance. In several jurisdictions, data protection authorities fall under ministries of information or security, raising structural concerns about

³⁷ The *African Charter* Art 9; *International Covenant on Civil and Political Rights* (1966) Art 19.

³⁸ Principle 42 of the *Declaration* (on personal data protection).

³⁹ Viljoen *International Human Rights Law* 370-375 (discussing the gap between regional standards and national implementation).

⁴⁰ Langa 2024 <https://www.theafricareport.com/354469/rise-of-chinese-surveillance-tech-in-africa-development-or-espionage/> (noting Huawei and ZTE involvement in smart-city surveillance and CCTV systems used to monitor dissidents and civil society across multiple African states).

⁴¹ Jili 2022 *Nature* 445-448 (discussing how African governments have integrated AI-powered systems into public security frameworks absent adequate regulation).

⁴² Amnesty International 2021 <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>.

⁴³ Human Rights Watch 2021 <https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses>.

their ability to constrain state surveillance practices.⁴⁴ The chilling effect is well-documented, and as a result, individuals avoid political expression online, restrict associational activities, or self-censor for fear of retribution.⁴⁵ Harm moves from abstract risk to actual impacts on constitutional rights.⁴⁶

2.2 *Digital constitutionalism and human rights*

The study of surveillance has moved from describing how states watch their citizens to asking what law can do about it. Early sociological work mapped the mechanisms of control,⁴⁷ later scholarship turned to the legal and governance questions that algorithmic power raises.⁴⁸ African surveillance complicates both moves. The technologies are procured from foreign vendors, which means external commercial and political priorities are embedded in domestic security practice the moment a contract is signed. The state that operates the surveillance is not the actor that designed it, and the law that governs the operation rarely reaches the design.⁴⁹

This complicates the dominant Western theoretical accounts. Zuboff's surveillance capitalism describes the corporate commodification of personal data in advanced market democracies and is partially applicable to private African surveillance, including the South African Vumacam network analysed below.⁵⁰ It does not, however, capture the predominant African pattern in which governments use the same technologies to consolidate political authority, for which the framing of digital authoritarianism is closer to the ground.

Human rights law sets the normative benchmarks that surveillance practice should meet. Surveillance measures must satisfy the requirements of legality and necessity to be defensible.⁵¹ The *African Charter* does not explicitly protect digital privacy, but *ICCPR* Article 17 supplies the analogy that evolving regional interpretation has accepted.⁵² Declarations by the ACHPR Special Rapporteur on Freedom of Expression further reinforce internet freedom and digital rights (2016 and 2019).⁵³

Despite these norms, systemic implementation gaps exist. Research consistently highlights that African states fall short on enforcement and

⁴⁴ Access Now 2025 <https://www.accessnow.org/press-release/africa-keepiton-internet-shutdowns-2024/>.

⁴⁵ Stevens *et al* 2023 *Big Data & Society*.

⁴⁶ Nwafor 2021 *IJLIT* 225-240.

⁴⁷ Foucault *Discipline and Punish*.

⁴⁸ Zuboff *Age of Surveillance Capitalism*.

⁴⁹ Couldry and Mejias 2019 *Internet Policy Review*.

⁵⁰ Feldstein "Surveillance in the Illiberal State" 351-364.

⁵¹ De Hert and Gutwirth 2006 *CLSR* 61-104.

⁵² The *Declaration* Art 9; *International Covenant on Civil and Political Rights* (1966) Art 17.

⁵³ Principles 41-42 of the *Declaration*.

delegate broad discretionary authority to executive actors. Studies by Privacy International⁵⁴ and Access Now⁵⁵ document how these deficiencies undermine meaningful oversight and weaken rights protections in practice.

Constitutionalising digital rights is the response most often proposed in the literature on AI governance, on the theory that constitutional entrenchment gives privacy and algorithmic accountability protections a stronger legal footing and a clearer basis for judicial review than ordinary statute can provide.⁵⁶ Whether that theory holds in practice is precisely the question this article examines. South Africa and Nigeria have both taken steps in this direction, yet they differ in enforcement capacity and interpretive jurisprudence. The variation is what makes the comparison productive.

2.3 Data colonialism and procurement activity

Surveillance governance in Africa cannot be analysed without attending to who builds the systems, who owns them, and who controls the data they generate. These questions are not contractual details. They determine what African law can realistically demand from AI surveillance, because vendor dependence and extraterritorial control shape the operational reality that law must engage with.

Couldry and Mejias name the broader phenomenon.⁵⁷ Data colonialism is the extraction and commodification of human life through digital infrastructures, enabled by surveillance-capable technologies that expand globally without corresponding protections or political agency for the populations they monitor.⁵⁸

The African case sharpens the critique. Foreign entities fund, install, and maintain much of the surveillance infrastructure that African states use. Chinese state-backed firms such as Huawei supply hardware, and Western technology companies offer cloud infrastructure for secure data storage. Public-private surveillance partnerships in this configuration are not neutral procurement relationships. They subordinate national data governance to

⁵⁴ Privacy International 2023 <https://privacyinternational.org/examples/5291/report-finds-african-countries-adopt-digital-surveillance-despite-human-rights-threat>.

⁵⁵ Access Now 2025 https://media.licdn.com/dms/document/media/v2/D4E1FAQHO-28C-2Wxlw/feedshare-document-pdf-analyzed/B4EZjNIFNxHoAc-/0/1755795712763?e=1767830400&v=beta&t=U3oaVP0wHzM7zlevRgaRwAryb_YT5BbF25j7ZRaEpGQ&acrobatPromotionSource=linkedin_chrome-post_view.

⁵⁶ Access Now 2025 https://media.licdn.com/dms/document/media/v2/D4E1FAQHO-28C-2Wxlw/feedshare-document-pdf-analyzed/B4EZjNIFNxHoAc-/0/1755795712763?e=1767830400&v=beta&t=U3oaVP0wHzM7zlevRgaRwAryb_YT5BbF25j7ZRaEpGQ&acrobatPromotionSource=linkedin_chrome-post_view.

⁵⁷ Couldry and Mejias 2019 *Internet Policy Review* 1-20.

⁵⁸ Couldry and Mejias 2019 *Internet Policy Review* 1-20.

corporate priorities and the regulatory regimes of the supplier's home jurisdiction.

Domestic legal frameworks are not built to regulate these arrangements. Sensitive biometric and behavioural data flow through systems that no African regulator can fully audit, and the result is diminished local control over the most consequential categories of personal information.⁵⁹ Ensuring AI sovereignty in this environment requires laws that enforce local data processing, mandate disclosure of surveillance contracts, and establish a national review of foreign technology standards.⁶⁰

The Ugandan and Kenyan deployments show what happens when these mechanisms are absent. Uganda's Safe City Project and Kenya's Integrated Command, Control and Communication system operate as forms of techno-authoritarianism enabled by geopolitical influence and weak domestic safeguards, and both function in legal grey zones.⁶¹

The pattern is not unique to these two countries. Many African states have surveillance laws that import elements from the *General Data Protection Regulation* (GDPR)⁶² or the *US Patriot Act*,⁶³ without the institutional mechanisms to enforce the rights those laws describe. Donor-driven legal reform has compounded the problem by incentivising compliance-based surveillance regulation⁶⁴ that emphasises formal regulation over democratic legitimacy.⁶⁵

This is why data sovereignty and procurement transparency belong in constitutional analysis rather than in administrative law alone. The information asymmetries that vendor dependence creates are precisely what Pasquale's black box framework names, and in African jurisdictions, the opacity is doubled, layered on both the technology and the sovereign actors that deploy it, as examined in the next section.

⁵⁹ Ademuyiwa and Adeniran 2020 https://www.cigionline.org/sites/default/files/documents/no244_0.pdf.

⁶⁰ Ademuyiwa and Adeniran 2020 https://www.cigionline.org/sites/default/files/documents/no244_0.pdf.

⁶¹ Access Now 2024 <https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf> (avoid independent audits or human rights scrutiny, ostensibly framed as crime prevention or urban management tools but rarely subjected to independent audits or human rights scrutiny).

⁶² *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L119/1.

⁶³ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* 115 Stat 272 (2001) (*US Patriot Act*).

⁶⁴ De Gregorio and Dunn 2022 *CMLR*.

⁶⁵ Brown and Marsden *Regulating Code*.

2.4 Pasquale's Black Box problem

Pasquale's Black Box Society offers the framework that anchors the algorithmic sovereignty gap.⁶⁶ The book examines how algorithmic decision-making in finance, healthcare, and law enforcement is shielded from scrutiny by proprietary protections, technical complexity, and institutional secrecy. Pasquale identifies three layers of opacity. First, the technical question of how the system works; second, the operational question of how decisions are made; and third, the institutional question of who has the power to oversee or intervene.

African surveillance contexts expose what each layer means in practice. Individuals subjected to algorithmic profiling, location tracking, or biometric matching usually receive no notice of how or why they were targeted, leaving due process, administrative fairness, and effective legal remedies without operational content.⁶⁷ As Pasquale's framework shows, technological inscrutability creates a democratic deficit, where public authorities exercise significant coercive power without meaningful transparency or accountability.⁶⁸ The deficit is amplified in environments where judicial oversight is constrained and where public access to government information is limited. Some African jurisdictions tend to combine all three.

Pasquale's framework is useful here because it explains a specific mechanism rather than describing a general failure. Algorithmic opacity disables the ordinary legal safeguards (notice, review, remedy) that surveillance law assumes will function, and Pasquale identifies the concrete legal tools that can restore them.

Pasquale advocates explainability standards, independent audits, and rights to human review, which align with broader movements in algorithmic accountability⁶⁹ and digital constitutionalism.⁷⁰ These interventions require that AI surveillance systems be designed and deployed to allow affected individuals and oversight bodies to interrogate and contest algorithmic decisions.⁷¹ In African contexts, embedding such safeguards into national surveillance laws is essential to satisfy constitutional protections for privacy, equality and fair trial and to meet regional human rights obligations under instruments such as the *African Charter*.

⁶⁶ Pasquale *Black Box Society*.

⁶⁷ Adeola and Mutua *Palgrave Handbook of Democracy*.

⁶⁸ Pasquale *Black Box Society*.

⁶⁹ Wachter, Mittelstadt and Russell 2017 *Harv J L & Tech* 841.

⁷⁰ De Gregorio and Radu 2022 *IJLIT* 68-87.

⁷¹ De Gregorio and Radu 2022 *IJLIT* 68-87.

Read into postcolonial conditions, Pasquale's framework⁷² reveals something his original analysis does not address. The opacity that surveillance produces is layered on top of foreign vendor ownership of the technology and the data. The state that deploys the system cannot fully audit it. The regulator that should hold the state accountable cannot reach behind the vendor's proprietary protections. The citizen affected by the system encounters two black boxes rather than one. The algorithmic black box Pasquale describes, and the sovereign black box created by vendor dependence. The sovereign black box is the structural condition in which the state operating a surveillance system has less technical knowledge of that system than the foreign vendor that built it, and in which neither domestic regulators nor courts have legal authority to compel disclosure across that boundary. The two reinforce each other. This expansion of Pasquale's framework establishes the algorithmic sovereignty gap as the lens through which African AI surveillance law must be evaluated and reformed.

3 Methods

3.1 Sample and case selection

This study uses a qualitative content analysis approach to examine AI-enabled surveillance governance in South Africa and Nigeria. These jurisdictions were selected because they represent diverse yet influential models of surveillance law in Africa. South Africa and Nigeria were selected as comparative cases because they combine constitutional rights frameworks with investments in AI-enabled surveillance and ongoing legal debates about digital governance. Both jurisdictions have enacted data protection legislation and maintain formal oversight structures, but they differ in their legal traditions, institutional capacities, and enforcement practices. This combination allows for structured comparison while avoiding assumptions of uniformity across African states.

South Africa has a post-apartheid constitution that provides strong protections for privacy, equality, and administrative justice, alongside a mature data-protection statute that is tested against interception laws.⁷³ Nigeria combines expansive interception and cybercrime powers with a newly enacted national data-protection statute, reflecting a regulatory environment shaped by colonial legal legacies, state security priorities, and contemporary technological adoption.⁷⁴

From an AI surveillance perspective, both countries have recently adopted advanced technologies (facial recognition systems deployed in

⁷² Pasquale *Black Box Society*.

⁷³ *Protection of Personal Information Act* 4 of 2013 (POPIA).

⁷⁴ *Nigeria Data Protection Act, 2023* (the NDPA); Nwafor 2024 AJLS 249-270.

Johannesburg⁷⁵ to the biometric voter and SIM registration databases in Nigeria⁷⁶), positioning them as strong case studies for understanding the governance challenges posed by algorithmic opacity and data colonialism in the African context.

The analysis draws on constitutional texts, primary legislation governing surveillance, policing, data protection and national security, as well as implementing regulations, policy documents, and publicly available enforcement materials. Sources were selected based on their relevance to AI-enabled surveillance, algorithmic decision-making, biometric systems, and accountability mechanisms.

Primary legal texts were selected purposively from government portals and legal databases (e.g., AfricanLII, Data Protection Africa and ministry websites) because the research objective was to analyse the substantive legal architecture governing surveillance, not to generate a representative sample of the broader legal corpus.

Using Dedoose software the analysis combines doctrinal legal interpretation with thematic coding of provisions against five governance dimensions: (1) Surveillance Authorisation: provisions authorising or constraining state surveillance powers; (2) Data and AI Regulation: rules governing data processing, biometric systems, or AI-driven analytics; (3) Accountability Mechanisms: institutional checks including judicial review and parliamentary reporting; (4) Risk Recognition: acknowledgment of AI-specific risks including algorithmic opacity, bias, or automated decision-making; and (5) Protections for Marginalised Groups: safeguards addressing discrimination or disproportionate surveillance impacts. The framework is my construct, developed from the digital constitutionalism literature reviewed above, and is offered as an analytical heuristic rather than as a validated coding instrument.

Civil society reports from Privacy International, Access Now, Amnesty International and Human Rights Watch (2013-2024), and reporting from investigative outlets including AmaBhungane and Premium Times were used as triangulation sources to evidence implementation gaps⁷⁷ and lived impacts.⁷⁸ The timeframe was restricted to enable comparability across the

⁷⁵ Sizwe Africa 2023 <https://www.itweb.co.za/article/digital-transformation-facial-recognition-technologies-anticipated-to-grow-despite-slowness-economic-growth/KWEBBvyLKPqgmRjO>.

⁷⁶ Federal Ministry of Communications and Digital Economy 2021 <https://nitda.gov.ng/wp-content/uploads/2021/05/REVISED-NATIONAL-DIGITAL-IDENTITY-POLICY-ON-SIM.pdf>.

⁷⁷ Robinson 2023 <https://www.ids.ac.uk/news/african-nations-spending-1bn-a-year-on-harmful-surveillance-of-citizens/>.

⁷⁸ Kwet 2022 <https://saiia.org.za/research/the-city-surveillance-state-inside-johannesburgs-safe-city-initiative/>.

two cases. Interpretive consistency was maintained through iterative re-reading of source materials.⁷⁹

The comparative analysis is intended to be primarily diagnostic and normative. Rather than offering statistically generalisable claims, the article uses these cases to highlight recurring legal-technical gaps and governance tensions that are likely to arise in other postcolonial contexts reliant on foreign surveillance technologies.

The study has two limitations. The two-case design narrows the evidence base, and solo coding limits inter-rater validation. Comparative analysis across additional African jurisdictions and empirical evaluation of audit and impact-assessment mechanisms in practice would strengthen the case for hybrid governance.

4 Results: Country-specific analysis

4.1 Nigeria

4.1.1 Overview of Nigeria's surveillance legal architecture

Nigeria's surveillance architecture has evolved from colonial and military-era controls into a dense statutory framework primarily focused on security.⁸⁰ Nigeria's surveillance framework is anchored in section 37 of the 1999 *Constitution*, which guarantees the privacy of citizens' homes, correspondence, telephone conversations and telegraphic communications.⁸¹ Surveillance authority is also distributed across multiple statutes. These include the *Nigerian Communications Act*, 2003,⁸² the *Lawful Interception of Communications Regulations*, 2019 under the *Nigerian Communications Act*,⁸³ and the *Cybercrimes (Prohibition, Prevention, etc.) Act*, 2015.

Judicial interpretation has played a decisive role in sustaining this security-oriented framework. Notably, the High Court upheld the constitutionality of regulation 8(2)(a) and (c) of the *Enforcement Process Regulations*, 2019, which permits authorities to access subscriber "basic information" without a warrant, invoking the security justification outlined in section 45 of the *Constitution*. Section 45 grants law enforcement broad powers to intercept and record electronic communications in ex parte proceedings without adversarial representation.

⁷⁹ Lungu 2022 *American Journal of Qualitative Research* 232-237.

⁸⁰ Nwafor 2024 *AJLS*.

⁸¹ *Constitution of the Federal Republic of Nigeria*, 1999 s 37.

⁸² *Nigerian Communications Act*, 2003 s 157.

⁸³ *Lawful Interception of Communications Regulations*, 2019.

Nigerian courts have confined their analysis to formal questions of statutory validity and constitutional permissibility. They have not engaged with the technical design or systemic risk profiles of surveillance technologies. As a result, AI-enabled surveillance remains somewhat insulated from challenges. The constitutional framework permits surveillance in principle but supplies few mechanisms to constrain it in practice, particularly where judicial oversight is procedurally limited, and safeguards against disproportionate impacts on marginalised groups are absent.

4.1.2 Surveillance-relevant legislative amendments and implications

Recent legislative amendments deepen the imbalance between surveillance powers and weak institutional constraints. Nigeria's *Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024* represents one of the most significant legislative interventions in the country's digital governance since its original enactment in 2015.⁸⁴ Several provisions⁸⁵ materially expand state capacity to monitor, store and access citizens' digital communications without procedural safeguards mandated by Principle 40 of the *Declaration* or Article 9 of the *African Charter*.⁸⁶

Section 21(3) is the most procedurally significant change in the *Amendment Act*, shortening the mandatory reporting window for cyber incidents from 7 days after occurrence to 72 hours after detection.⁸⁷ The provision requires public and private organisations to report cyber incidents to the National Computer Emergency Response Team (CERT) through sectoral CERTs or Security Operations Centres (SOCs). The text does not itself mandate automated detection. However, the shortened window creates strong incentives for organisations to deploy automated anomaly-detection systems. Moreover, the National CERT infrastructure that receives the reports operates with limited transparency about how submitted data is retained or shared with security agencies. The shift from a 7-day occurrence-based window to a 72-hour detection-based window accelerates state access to incident data while leaving the automated systems that produce that data outside any statutory disclosure or contestability requirement.⁸⁸

Section 38(1) mandates long-term mass data retention, requiring service providers to retain specific traffic data and subscriber information for at least 2 years.⁸⁹ Though framed with references to the *Nigerian Data Protection*

⁸⁴ *Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024* (*Cybercrimes Amendment Act*); Nwafor 2024 AJLS.

⁸⁵ *Cybercrimes Amendment Act* ss 21(3) and 38(1).

⁸⁶ Principle 40 of the *Declaration*; Art 9 of the *African Charter*.

⁸⁷ *Cybercrimes Amendment Act* s 21(3).

⁸⁸ *Cybercrimes Amendment Act* s 21(3).

⁸⁹ *Cybercrimes Amendment Act* s 38(1).

Act (NDPA), this provision establishes a default mass surveillance infrastructure. The provision does not establish meaningful independent oversight, leaving access to retained data at the discretion of security agencies.⁹⁰ There is no evidence of routine independent audits or ex post review of how retained data is queried or analysed.

Under this article's coding framework, section 38(1) constitutes an explicit Surveillance Authorisation, as it directly obliges providers to retain and supply user data. It also reflects explicit data and AI regulation, as it links to statutory rules governing data protection, albeit weakly enforced. However, Accountability Mechanisms are absent, as no independent review structures are mandated. Finally, Protections for Marginalised Groups are only implicit, given that while data protection principles are invoked, there are no explicit safeguards addressing discrimination or the disproportionate impacts of surveillance.

Sections 22(1), 27(2) and 30 expand the explicit Institutional Reach, compelling private and public organisations to cooperate with the state on monitoring and integrating AI-driven financial surveillance across sectors. These provisions expand the scope of the entities required to cooperate with state data requests. Section 41's mandate for sectoral CERTs and SOCs creates centralised state-linked AI security infrastructures capable of ingesting public and private data flows.

4.1.3 *Nigeria Data Protection Act, 2023*

The *NDPA, 2023* explicitly addresses data-subject rights, including a right not to be subject to a decision based solely on automated processing (section 37) and transparency obligations (including notice of automated profiling). The *NDPA* also contains broad carve-outs. Numerous protections "shall not apply" to competent authorities processing personal data for criminal justice, national security and similar purposes, and an explicit statutory exemption pathway that enables state surveillance practice to persist under the guise of security.⁹¹

On paper, the *NDPA* is forward-looking. Section 37 recognises automated decision-making and grants data subjects the right not to be subject to solely automated decisions, while the obligations require controllers to inform data subjects about the existence and significance of automated processing.⁹²

Under the coding framework, this reflects explicit engagement with the Risk Recognition and Protections for Marginalised Groups codes. However, these protections are qualified by exceptions (e.g., when decisions are

⁹⁰ *Cybercrimes Amendment Act* s 38(1).

⁹¹ *NDPA* s 3(2)(a)-(c).

⁹² *NDPA* s 37.

authorised by a written law with safeguards or with data-subject consent).⁹³ The statutory carve-outs for "competent authorities" narrow operations to instances of "justified national security".⁹⁴

The operational reality of these carve-outs is evident in the government's NIN-SIM linkage policy, which mandates integrating citizens' national ID numbers with their mobile SIM registrations.⁹⁵ The NIN-SIM policy directly conditions mobile access on state-mandated identity linkage. It establishes no standalone data protection rules, provides no independent review or redress mechanism, and offers no targeted safeguards for the rural, low-income, and less digitally connected populations that mass disconnections disproportionately impact.⁹⁶

Despite the scale of these impacts, there are no documented compliance assessments and no accessible mechanism for affected individuals to challenge the law's proportionality. This enforcement silence shows us the gap between statutory rights and practical enforceability.

Investigative reports show that Nigerian security agencies have used foreign-built spyware to intercept calls and track device locations without public disclosure.⁹⁷ The case reflects dynamics often associated with data colonialism, where dependence on foreign surveillance technologies combines with broad statutory exemptions to limit transparency and public accountability. Such cases exemplify the sovereign black box dynamic theorised in this study, where technical opacity can shield surveillance practices from oversight.⁹⁸ Notably, these capabilities were introduced through security-sector procurement and vendor contracts rather than through explicit legislative debate or technology-specific authorisation.

4.1.4 *Pasquale's black box problem in the Nigerian context*

Nigeria's surveillance regime exhibits operational and institutional opacity, producing a compounded "black box". Technical opacity arises when surveillance systems process large volumes of communications and behavioural data without disclosing algorithms, training datasets, or error rates, etc. Section 21(3) of the *Cybercrimes (Prohibition, Prevention, etc.) Act*, 2015, empowers anomaly detection systems to flag potential threats

⁹³ NDPA s 37.

⁹⁴ NDPA s 37.

⁹⁵ Roberts 2025 <https://www.ids.ac.uk/publications/understanding-digital-rights-definitions-conceptions-and-myths/>.

⁹⁶ Roberts 2025 <https://www.ids.ac.uk/publications/understanding-digital-rights-definitions-conceptions-and-myths/>.

⁹⁷ Al Jazeera 2020 <https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report>.

⁹⁸ Al Jazeera 2020 <https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report>.

and trigger incident reports automatically; however, the manner in which they operate is inaccessible to citizens or even to courts for adjudication.

Operational opacity is further reinforced through *ex parte* warrant applications or metadata collection without judicial authorisation, so people are unaware when surveillance occurs.⁹⁹ Institutional opacity compounds the black box problem. Oversight is primarily assigned to agencies structurally linked to national security, such as the Nigerian Communications Commission, and competent authorities under the *NDPA*, which limits their ability to audit AI systems or sanction misuse.

Dependence on foreign technologies expands these gaps, as proprietary systems from companies such as Palantir and NSO Group prevent regulators from accessing source code or system architecture.¹⁰⁰ Evidence of technical, operational, and institutional opacity forms a "triple black box" that undermines constitutional protections.¹⁰¹ Coding results show explicit Surveillance Authorisation and moderate Data/AI Regulation, but absent Accountability Mechanisms and weak or absent Protections for Marginalised Groups.

4.1.5 Data colonialism and structural dependency

Nigeria's AI surveillance regime exemplifies the logic of data colonialism in practice.¹⁰² The state's capacity to monitor citizens relies heavily on foreign technologies and cloud-hosted storage of the national ID and SIM card database.¹⁰³ These arrangements create a structural dependency. While Nigerian agencies may operate these systems, they do not fully control software updates, proprietary algorithms or data processing pipelines.¹⁰⁴ Consequently, domestic regulators cannot independently mandate audit algorithms or implement bias mitigation measures, resulting in a deficit in algorithmic sovereignty.¹⁰⁵

This dependency operates on two levels. Legally, Nigeria's data protection framework permits broad cross-border transfers without effective extraterritorial enforcement; operationally, foreign vendors retain control

⁹⁹ *Cybercrimes (Prohibition, Prevention, etc) Act*, 2015 (the *Cybercrimes Act*).

¹⁰⁰ Al Jazeera 2020 <https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report>.

¹⁰¹ *Constitution of the Federal Republic of Nigeria*, 1999 s 37.

¹⁰² Couldry and Mejias 2019 *Television & News Media* 336-349.

¹⁰³ Al Jazeera 2020 <https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report>; Hillman and McCalpin 2019 <https://www.csis.org/analysis/watching-huaweis-safe-cities>.

¹⁰⁴ *Cybercrimes Act* s 21(3).

¹⁰⁵ *Cybercrimes Act* s 21(3).

over the infrastructure and software on which surveillance depends.¹⁰⁶ Vendor and geopolitical interests constrain the state's governance choices.¹⁰⁷

4.1.6 *Synthesis: The legal-technical gap*

The Nigerian case highlights the distance between formal legal protections and the realities of surveillance practice. Laws such as the *NDPA* and the *Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act, 2024*, adopt the language of privacy and accountability, yet broad security exemptions and weak oversight mechanisms continue to limit enforcement in practice. Surveillance capabilities are expanding through procurement agreements that receive little public scrutiny, while regulators often lack the technical access needed to examine how these systems operate. Legal safeguards coexist with surveillance practices that are difficult to challenge through existing institutional frameworks.

4.2 *South Africa*

4.2.1 *Overview of South Africa's surveillance legal architecture*

South Africa's surveillance architecture is quickly growing. As of February 2024, Gauteng has deployed nearly 7,000 surveillance cameras equipped with facial recognition technology,¹⁰⁸ including approximately 6,000 Vumacam-operated cameras, as well as access to an additional 5,000 partner cameras across the province and nationwide.¹⁰⁹ This expansion has occurred primarily through procurement arrangements and public-private partnerships. As a result, deployment has outpaced clear statutory standards governing proportionality and accountability.

The Gauteng Department of e-Government is also involved, emphasising its mandate to use technology to support the immediate fight against crime, corruption, vandalism and lawlessness.¹¹⁰ South Africa's approach to surveillance is more constitutionally advanced than that of many other African countries, rooted in section 14 of the Bill of Rights, which protects privacy, including personal communications and data.¹¹¹ This constitutional right is operationalised through the *Regulation of Interception of*

¹⁰⁶ See *NDPA* ss 41-43 (cross-border transfer provisions permitting broad exceptions and lacking extraterritorial enforcement); Feldstein *Rise of Digital Repression* (on Huawei safe-city deployments in Africa).

¹⁰⁷ Couldry and Mejias 2019 *Television & News Media*.

¹⁰⁸ Mokwena 2024 <https://briefly.co.za/southafrica/180039-gauteng-premier-panyaza-lesufi-launches-7000-facial-recognition-cameras/>.

¹⁰⁹ Brouwers 2024 <https://www.moneyweb.co.za/news/companies-and-deals/vumacam-announces-crime-fighting-partnership-with-gauteng-government/>.

¹¹⁰ Brouwers 2024 <https://www.moneyweb.co.za/news/companies-and-deals/vumacam-announces-crime-fighting-partnership-with-gauteng-government/>.

¹¹¹ Section 14 of the *Constitution of the Republic of South Africa*, 1996.

Communications and Provision of Communication-Related Information Act 70 of 2002 (*RICA*) and section 71 of the *Protection of Personal Information Act* 4 of 2013 (*POPIA*), establishing statutory interception and data protection, with explicit warrant requirements and rights-based limits on automated profiling.¹¹²

However, a close analysis reveals that formal legal structures do not fully translate into enforceable protections. The Constitutional Court's judgment in the *AmaBhungane* case found *RICA* deficient in five critical respects. The absence of post-surveillance notification; inadequate judicial independence of the designated judge appointed by the Minister of Justice; insufficient protection for privileged communications between lawyers and clients and between journalists and their sources; weak management and storage of intercepted information; and the finding that the bulk interception regime conducted by the State Security Agency's National Communications Centre was unlawful because it was not authorised by any law. The fifth finding is particularly significant because it ended state bulk surveillance with no further parliamentary action required.¹¹³

Legislative attempts to address these gaps, such as the 2023 *RICA Amendment Bill*, were returned to Parliament by President Ramaphosa on 15 November 2024.¹¹⁴ This has left core defects intact, most notably indefinite notification deferrals, no procedural review for withholding notice, and continued ex parte authorisations without a public advocate.¹¹⁵ While the Constitutional Court has articulated robust privacy principles, these judgments have not yet translated into enforceable constraints on the procurement or deployment of AI-enabled surveillance systems, leaving significant discretion at the operational level.

The evaluation of the substantive safeguards confirms some coding patterns. The *necessity* principle remains under-enforced. *RICA* does not mandate that interception occur only as a last resort after less intrusive measures have failed. *Proportionality* is undermined by the metadata "backdoor" in section 205 of the *Criminal Procedure Act*, which allows access to sensitive communications data through a parallel, less accountable process that circumvents *RICA*'s formal protections.¹¹⁶ Though

¹¹² *Regulation of Interception of Communications and Provision of Communication-Related Information Act* 70 of 2002 (*RICA*); *POPIA* s 71.

¹¹³ *AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC* 2021 3 SA 246 (CC) (the *AmaBhungane* case).

¹¹⁴ The Presidency 2024 <https://www.thepresidency.gov.za/president-ramaphosa-refers-rica-amendment-bill-national-assembly>.

¹¹⁵ The Presidency 2024 <https://www.thepresidency.gov.za/president-ramaphosa-refers-rica-amendment-bill-national-assembly>.

¹¹⁶ *Criminal Procedure Act* 51 of 1977 s 205.

judicially anchored, oversight is structurally compromised by executive-influenced appointments and reliance on one-sided state evidence.¹¹⁷

National security exceptions and procedural loopholes, such as indefinite notification deferrals, allow authorities to bypass both notification and disclosure requirements.¹¹⁸ These outcomes confirm that South Africa's legal framework fails to effectively regulate the operational deployment of AI-enabled surveillance, resulting in a persistent legal-technical gap.

4.2.2 Surveillance-relevant legislative amendments and implications

In South Africa surveillance oversight is formally vested in the judiciary and the Information Regulator. However, executive influence over judicial appointments and structural limitations on the regulator constrain meaningful review. Statutory remedies exist, as demonstrated in *AmaBhungane*, yet national security exceptions and procedural loopholes substantially weaken their practical effect.¹¹⁹ Section 71 of *POPIA* introduces procedural safeguards and notice obligations for automated decision-making, but broad exemptions for law enforcement and national security significantly dilute their operational impact.¹²⁰

The practical consequences of these legislative gaps are illustrated in *Vumacam (Pty) Ltd v Johannesburg Roads Agency*. Vumacam (Pty) Ltd, a private operator of approximately 6,000 CCTV cameras across Gauteng, applied to the High Court after the Johannesburg Roads Agency suspended its wayleave applications on the basis that the surveillance network raised privacy concerns.¹²¹ The High Court ruled in Vumacam's favour, holding that the Johannesburg Roads Agency's mandate was limited to road infrastructure and did not include the authority to refuse wayleaves on privacy grounds.¹²² The court did not adjudicate whether the surveillance itself was constitutionally compliant. It held that privacy regulation was a matter for legislation and for bodies with appropriate mandates, not for a road authority acting through its wayleave function.¹²³

The case is significant for the present analysis precisely because it demonstrates the institutional gap the article identifies. An administrative

¹¹⁷ *Criminal Procedure Act* 51 of 1977 s 205.

¹¹⁸ *Criminal Procedure Act* 51 of 1977 s 205.

¹¹⁹ The *AmaBhungane* case. Also see *RICA*.

¹²⁰ *POPIA* s 71.

¹²¹ *Vumacam (Pty) Ltd v Johannesburg Roads Agency* (14867/20) [2020] ZAGPJHC 186 (20 August 2020). See also Nash 2022 <https://www.biometricupdate.com/202204/a-2020-court-fight-in-south-africa-reveals-dominance-of-biometric-surveillance-industry>.

¹²² Nash 2022 <https://www.biometricupdate.com/202204/a-2020-court-fight-in-south-africa-reveals-dominance-of-biometric-surveillance-industry>.

¹²³ Nash 2022 <https://www.biometricupdate.com/202204/a-2020-court-fight-in-south-africa-reveals-dominance-of-biometric-surveillance-industry>.

body attempted to constrain private surveillance with the only tool available to it, and was correctly told that it was not the right one. No statutory or constitutional process has filled the gap, and Vumacam has continued to expand its network through procurement channels rather than through democratic authorisation of surveillance practice.¹²⁴

4.2.3 *Pasquale's black box problem in the South African context*

Applying Pasquale's framework¹²⁵ to South Africa's surveillance ecosystem reveals persistent opacity. Technical opacity is evident in AI-enhanced platforms such as Vumacam's iSentry analytics and imported facial recognition systems, where the algorithmic logic, training data, and error rates remain inaccessible to regulators and the public.¹²⁶ Operational opacity arises from ex parte warrant procedures and the lack of adversarial participation, which prevents targets from contesting the criteria or algorithmic decisions. Institutional opacity persists because oversight bodies, including the Information Regulator, lack the statutory authority to compel the disclosure of algorithmic models or to perform technical audits.

This "triple black box" demonstrates how formal legal protections coexist with enforcement practices that render them ineffective. Coding confirms explicit Surveillance Authorisation and Data/AI Regulation, but identifies absent or weak Accountability Mechanisms, Risk Recognition, and Protections for Marginalised Groups, showing how AI-mediated surveillance can expand with minimal constraint.

4.2.4 *Data colonialism and structural dependency*

South Africa's reliance on foreign surveillance technologies, including Australian-developed iSentry analytics, imported IMSI catchers, and cloud-based interception infrastructure, exemplifies state technical control by external vendors.¹²⁷ The state manages deployment; the software architecture and updates remain outside the domestic jurisdiction.

This arrangement produces legal "dead zones" where constitutional protections cannot be effectively enforced against foreign vendors, and contractual obligations prioritise vendors' intellectual property over

¹²⁴ Heywood and Pongweni 2023 <https://www.dailymaverick.co.za/article/2023-08-29-gauteng-crime-prevention-wardens-set-up-unlawfully-experts/>.

¹²⁵ Pasquale *Black Box Society*.

¹²⁶ *Vumacam (Pty) Ltd v Johannesburg Roads Agency* (14867/20) [2020] ZAGPJHC 186 (20 August 2020).

¹²⁷ Privacy International 2018 <https://privacyinternational.org/explainer/2222/imsi-catchers>; First Distribution date unknown <https://firstdistribution.com/our-brands/isentry/>; Gen N 2533 in GG 50741 of 31 May 2024 (National Policy on Data and Cloud).

transparency and public accountability.¹²⁸ This mirrors Nigeria's dependency dynamics. Coding these features reveals high scores for Data/AI Regulation and Surveillance Authorisation but low scores for Accountability Mechanisms and Risk Recognition, illustrating how infrastructural dependency reproduces opacity and selective enforcement in practice.

4.2.5 Synthesis: The legal-technical gap

South Africa exemplifies the tension between constitutional surveillance governance and the realities of foreign-dependent surveillance infrastructure. While the *Constitution* protects the right to privacy, and statutes like *RICA* and *POPIA* provide oversight frameworks, these rights are often undermined by institutional limitations.¹²⁹

Statutory frameworks like *RICA* and *POPIA*, along with section 205 of the *Criminal Procedure Act*,¹³⁰ establish legal avenues for surveillance. However, these laws often enable selective enforcement. For example, section 205 allows law enforcement to access metadata with minimal judicial oversight, potentially circumventing the more stringent requirements of *RICA*.¹³¹ Moreover, *POPIA*'s provisions on automated decision-making are undermined by broad exemptions for law enforcement and national security, diluting their effectiveness.¹³² These parallel legal regimes create a hybrid enforcement landscape where rights are formally recognised but can be selectively circumvented.¹³³

While section 71 of *POPIA* introduces procedural safeguards and notice obligations for automated decision-making, the absence of mandatory audit powers, procurement transparency and technical disclosure obligations means that advanced surveillance technologies operate largely beyond constitutional reach.¹³⁴ South Africa demonstrates that even with robust constitutional rights and judicial review, legal-technical gaps persist.¹³⁵

¹²⁸ Hao and Swart 2022 <https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid>.

¹²⁹ *POPIA* s 71; *RICA*.

¹³⁰ *Criminal Procedure Act* 51 of 1977 s 205.

¹³¹ Swart 2023 https://intelwatch.org.za/wp-content/uploads/2023/05/Intelwatch_Supplementary_report_Reforming_surveillance_in_South_Africa_May_2023.pdf.

¹³² *POPIA* s 71.

¹³³ Swart 2023 https://intelwatch.org.za/wp-content/uploads/2023/05/Intelwatch_Supplementary_report_Reforming_surveillance_in_South_Africa_May_2023.pdf.

¹³⁴ *POPIA* s 71.

¹³⁵ The *AmaBhungane* case.

5 Discussion

5.1 Vendor dependence as a governance mechanism

Figure 1 is a conceptual representation of the algorithmic sovereignty gap.

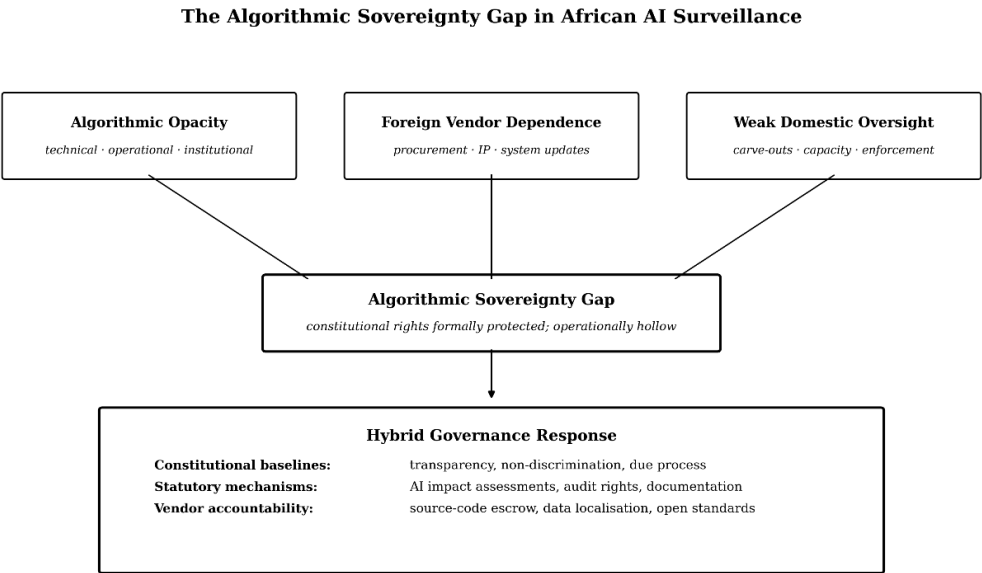


Figure 1 represents the algorithmic sovereignty gap. Three interlocking forces: algorithmic opacity, reliance on foreign vendors, and weak domestic oversight. This produces a structural disjunction between formal constitutional protections and operational surveillance practices. The hybrid governance response combines constitutional baselines with statutory and procurement-level mechanisms.

Addressing the algorithmic sovereignty gap in African AI surveillance governance needs a multidimensional, constitutionally grounded approach that integrates both legal and technical safeguards. A central issue relates to vendor dependence and cross-border data flows.¹³⁶

The cases show that surveillance capacity in both South Africa and Nigeria has expanded primarily through procurement contracts and public-private partnerships.¹³⁷ This procurement-led pathway allows AI-enabled surveillance systems to enter use without ex ante proportionality assessment or the enforcement capacity to monitor them.¹³⁸ Vendor dependence functions as a technical condition and a governance mechanism that reallocates regulatory authority away from domestic institutions.¹³⁹ Reports from Kenyan Safe-City projects,¹⁴⁰ Ethiopia's ZTE-

¹³⁶ Nwafor 2023 *South African Intellectual Property Law Journal* 88-92.
¹³⁷ Nwafor 2023 *South African Intellectual Property Law Journal* 88-92.
¹³⁸ Lungu "Enhancing Public Service Delivery" 188-204.
¹³⁹ Lungu "Enhancing Public Service Delivery" 188-204.
¹⁴⁰ Sheombar and Skelton "Who Supplies Digital Surveillance Technologies?" 183.

built telecom infrastructure,¹⁴¹ and Nigeria's adoption of Huawei facial recognition systems¹⁴² illustrate the same configuration across jurisdictions.

From a governance-engineering perspective, this is dangerous because it is unclear what is auditable and what is not. Proprietary systems are closed architectures, and trade-secret protections restrict meaningful technical inspection even where contracts permit oversight. Audit rights become high-level compliance checks.¹⁴³ Regulators without independent technical capacity often cannot negotiate procurement terms that would change this, and the result is that the governance of citizens' data is shaped by foreign corporate actors rather than domestic oversight.¹⁴⁴

This is data colonialism in operational terms, where historical power asymmetries are reproduced through modern technological infrastructure.¹⁴⁵ It is also, more narrowly, a procurement problem with a procurement solution. Mandatory third-party audits, source-code escrow, and enforceable standards for algorithmic explainability are the legal tools that can begin to close it,¹⁴⁶ and emerging proposals for blockchain-based procurement registries point toward additional auditability mechanisms at the pilot stage.¹⁴⁷

The hollowing-out effect this produces was visible in both South Africa and Nigeria. Constitutional and statutory protections formally exist but are undermined in practice by limited audit authority and the absence of ways to contest vendor-controlled systems.

5.2 Constitutionalising algorithmic governance

The scholarly debate over how to address this hollowing-out has divided the literature into two positions. The first holds that statutory and administrative reforms are insufficient because legislatures can weaken or repeal protections under political pressure,¹⁴⁸ and because AI systems mediate access to rights (due process, equal protection, sovereignty) that are traditionally protected at the constitutional level.¹⁴⁹

¹⁴¹ Human Rights Watch 2014 <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia>.

¹⁴² MSN 2025 <https://www.msn.com/en-xl/africa/nigeria/huawei-cloud-showcases-ai-potential-at-lagos-forum/ar-AA1KJd0x>.

¹⁴³ Herold *et al* 2023 *International Journal of Physical Distribution and Logistics Management* 424-447.

¹⁴⁴ Maepa, Mpwanya and Phume 2023 *Journal of Transport and Supply Chain Management*.

¹⁴⁵ Couldry and Mejias 2019 *Television & News Media*.

¹⁴⁶ Panya and Awuor 2023 *Strategic Journal of Business & Change Management* 1435-1456.

¹⁴⁷ Kademeteme and Bvuma 2023 *Journal of the British Blockchain Association*.

¹⁴⁸ Judge, Nitzberg and Russell 2025 *Policy and Society* 85-97.

¹⁴⁹ Lungu and McCue 2024 *Journal of AI Law and Regulation* 310-330.

The second position warns against embedding AI-specific principles into constitutional text because doctrine is rigid and slow to adapt. Hard-coding technical principles risks freezing contested approaches into inflexible frameworks, and asking courts to determine complex technological trajectories can be difficult. Statutory and regulatory mechanisms, on this view, are better suited to integrate technical expertise and iterative oversight.

The case analysis in this article supports a hybrid position rather than either domain. The South African and Nigerian evidence shows that statutory frameworks alone have not constrained AI-enabled surveillance, which weakens the case for relying solely on statutes. But the same evidence shows that the problems are technical and rapidly evolving (auditability, model documentation, bias evaluation), which weakens the case for resolving them at the constitutional level.

What the cases support is constitutional articulation of enduring principles (non-discrimination, due process, transparency in the exercise of public power) operationalised through statutory and procurement regimes that specify auditing, documentation, and technical compliance standards. Constitutionalisation secures the normative floor; statute and procurement carry the operational weight. Section 6 develops this hybrid model in detail.

5.3 Competing interpretations of surveillance governance

Three counterarguments to the analysis presented here merit engagement. The first is that surveillance is sometimes legitimately needed for security, and that the constitutional carve-outs reflect appropriate proportionality rather than failure. This article does not dispute the existence of legitimate security uses; it argues that the proportionality and oversight conditions that would make surveillance constitutionally defensible are systematically absent in the South African and Nigerian frameworks. The carve-outs in question authorise broad executive discretion without the procedural safeguards that proportionality analysis requires.

The second is that source-code escrow and data localisation may not be feasible given current trade and intellectual property regimes. This is a real constraint. The recommendations developed here are not intended to be immediately enforceable against foreign vendors under existing international law. They are offered as conditions that domestic procurement law can impose on contracts, with state-level leverage at the procurement stage providing the practical mechanism for enforcement. The literature¹⁵⁰ on procurement-stage regulation of AI systems supports this approach.

¹⁵⁰ Lungu "Enhancing Public Service Delivery" 188-204.

The third is that the pattern observed in South Africa and Nigeria reflects a global pattern of constitutional ineffectiveness against security-driven surveillance, rather than a postcolonial-specific phenomenon. The US exhibits similar patterns. This article does not claim the algorithmic sovereignty gap is unique to postcolonial contexts. It claims that postcolonial conditions intensify the gap by adding vendor asymmetry to opacity and weak oversight. The Northern frameworks of Pasquale and Couldry-Mejias do not fully describe this intensification; the extension developed here aims to fill that gap rather than to claim postcolonial exceptionalism.

6 Recommendations

6.1 *AI-specific legislative and procedural reform*

The algorithmic sovereignty gap cannot be closed at any single level of law. Constitutional protections set the right normative floor but cannot specify the technical mechanisms that opaque systems require. Statute can specify those mechanisms, but cannot bind the foreign vendors whose contracts determine what regulators are actually permitted to see. Procurement law can reach those vendors, but only at one moment (the point of contract), and only if a higher-tier authority makes the conditions enforceable. The hybrid model proposed here distributes the work across three tiers,¹⁵¹ each responsible for what the others cannot reach.

¹⁵¹ These tiers are interdependent. Tier 1 without Tier 2 leaves principles unenforced. Tier 2 without Tier 3 produces statutory rights that cannot be applied to vendor-controlled systems. Tier 3 without Tiers 1 and 2 reduces algorithmic governance to procurement bureaucracy. The model works as a unit or not at all.

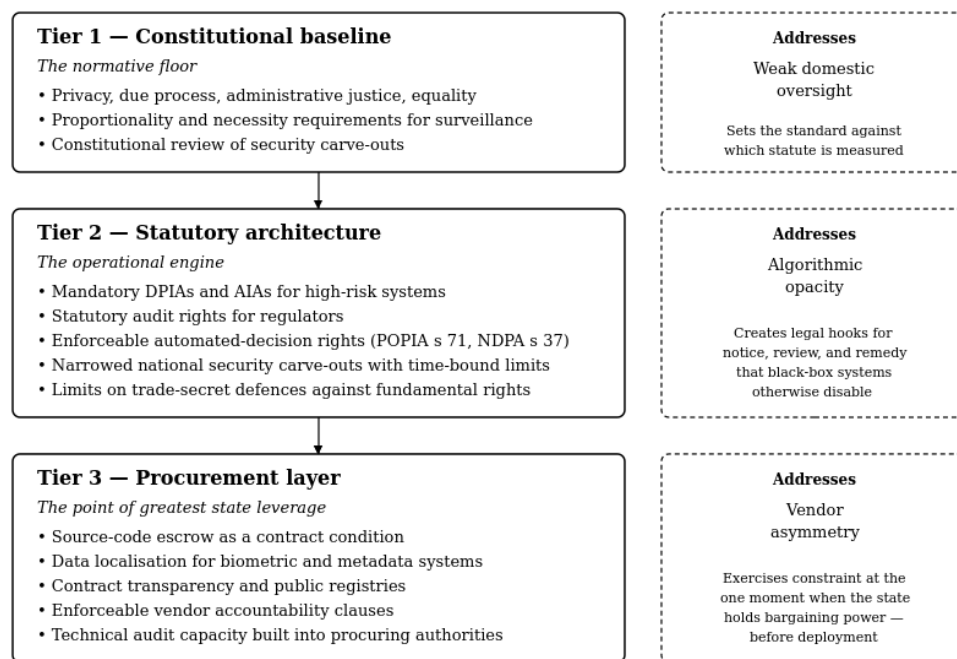


Figure 2: Three-tier hybrid governance model. Constitutional principles flow down into statute; statute is enforced through procurement. The three forces of the algorithmic sovereignty gap (weak oversight, opacity, vendor asymmetry) are addressed at the tier with matching authority.

Tier 1 is the constitutional baseline. The South African Bill of Rights and section 37 of the Nigerian *Constitution* already articulate the relevant principles (privacy, due process, administrative justice, equality), and regional instruments add the principles of proportionality and necessity. The work at this tier is not to add new constitutional text. Here there is a focus on making sure these existing principles are read as binding on security-driven surveillance, including where carve-outs purport to displace them. Constitutional review of those carve-outs enables the model to address weak domestic oversight at the structural level.

Tier 2 is the statutory architecture that operationalises these principles. Five elements carry the operational weight. First, standardised and publicly accessible data protection impact assessments and algorithmic impact assessments before deployment of high-risk surveillance systems. Second, enforceable rights to explanation of automated decisions, aligning with *POPIA* section 71 and *NDPA* section 37 and reflecting the global standard exemplified by GDPR Article 22.

Third, statutory audit rights for regulators that override trade-secret defences when fundamental rights are implicated. Fourth, narrowing of national security exceptions, currently expansive under *RICA* in South Africa and under the *Cybercrimes (Prohibition, Prevention, etc) Act, 2015*¹⁵²

¹⁵² The *Cybercrimes Act* (as amended in 2024) ss 21 and 38.

and *Lawful Interception of Communications Regulations*, 2019 in Nigeria.¹⁵³ This might be achieved through time-bound limitations and mandatory reporting to independent oversight bodies. Fifth, minimum standards for documentation and bias evaluation in high-risk systems, anchored in the algorithmic accountability literature.¹⁵⁴

Tier 3 is the procurement layer, and it is the most underutilised. Once a surveillance system is operational, technical opacity and contractual protections reduce what regulators can demand. Before the contract signature, the state holds more bargaining power. The procurement tier converts that leverage into enforceable conditions. This can look like source-code escrow with a domestic escrow agent, data localisation for biometric and metadata systems, public registries of surveillance contracts, vendor accountability clauses tied to the audit rights established at Tier 2, and (critically) funding for technical audit capacity within the procuring authority itself.

6.2 Application to South Africa

South Africa's most immediate work sits at Tier 2. The *RICA Amendment Bill*, referred back to Parliament in November 2024, leaves the constitutional defects identified by the Constitutional Court in *AmaBhungane* largely unaddressed: indefinite notification deferrals, no procedural review for withholding notice, and continued ex parte authorisations without a public advocate. The amendment process is the natural vehicle for narrowing the national security carve-out, introducing time-bound limitations, and requiring particularised justifications.

A parallel statutory gap concerns audit authority. The Information Regulator has a substantive mandate under *POPIA* but lacks the technical audit power to inspect AI-driven surveillance systems operated by private actors such as Vumacam. The *Vumacam* decision was correct on its facts. The road authority is not a privacy regulator, yet it exposed the absence of any body with statutory authority to evaluate the privacy implications of a private 6,000-camera network. A statutory amendment granting the Information Regulator audit powers over high-risk private surveillance operators would fill this gap.

At Tier 3, South Africa's reliance on Australian-developed iSentry analytics, imported IMSI catchers, and cloud-based interception infrastructure illustrates the procurement-stage entry point precisely. Contract conditions imposed at acquisition (source-code escrow with a domestic agent, localised processing of biometric data, mandated technical disclosure) are

¹⁵³ *Lawful Interception of Communications Regulations*, 2019 (made under the *Nigerian Communications Act*, 2003).

¹⁵⁴ Mittelstadt *et al* 2016 *Big Data & Society*.

the practical mechanism for converting *POPIA*'s formal automated-decision protections into operational constraints on these specific systems.

6.3 Application to Nigeria

Nigeria's most pressing work also sits at Tier 2, but the centre of gravity is different. The *Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act, 2024* expanded interception and retention powers without corresponding procedural safeguards. Section 21's 72-hour incident-reporting window creates strong incentives for automated detection without statutory disclosure or contestability requirements; section 38's two-year mass retention requirement establishes a default surveillance infrastructure without independent oversight. Both provisions need amendment to introduce time-bound limits, particularised justifications, and audit reporting to a body operationally independent of the security agencies they oversee.

NDPA section 37 already provides a statutory hook for automated-decision rights, but its operational impact has been minimal in the surveillance context. Implementing regulations specifying notice obligations, explanation rights, and contestability procedures for AI-mediated security decisions would activate this provision. The *Lawful Interception of Communications Regulations, 2019* require parallel narrowing to align with the proportionality standards in regional instruments.

At Tier 3, Nigeria's biometric voter and SIM registration infrastructure, alongside its adoption of Huawei facial recognition systems, presents the same procurement-leverage opportunity South Africa has. Contract-stage conditions (escrow, localisation, audit rights, vendor accountability clauses) are where the model bites in practice.

6.4 Sequencing and feasibility

Not all elements of the model are equally actionable in the short term. Constitutional doctrine on the carve-outs (Tier 1) takes time. Statutory amendment (Tier 2) is achievable within an electoral cycle but depends on political will, particularly for narrowing security exceptions. Procurement reform (Tier 3) is the most immediately tractable because it operates through executive and administrative authority that does not always require fresh legislation; contract conditions, public registries, and audit capacity can be introduced through procurement regulations and standing instructions to procuring authorities.

The practical implication is that the procurement tier should not wait for the upper tiers to be complete. Each escrow clause, each localisation requirement, each transparency obligation imposed at procurement adds constraint to the operational environment in which Tier 2 statutory reforms will later be applied. The strongest case for sequencing reform from the

bottom up is that Tier 3 is where the gap was widening fastest in both jurisdictions throughout the period this study examines, and where domestic authority is least constrained by international law.

7 Conclusion

This article has made two contributions to the literature on AI surveillance governance in postcolonial contexts. The theoretical contribution is the concept of the algorithmic sovereignty gap, which names the structural disconnection between constitutional protections and the operational realities of vendor-controlled infrastructure. The prescriptive contribution is a hybrid governance model that anchors transparency and accountability in constitutional baselines while operationalising them through statutory, procurement, and audit mechanisms. Closing the gap requires more than legislative reform. South Africa's most immediate priority is the unresolved *RICA* amendments and the absence of statutory audit authority over private operators. Nigeria's most pressing work is to narrow the *Cybercrimes Act's* expansive interception provisions and operationalise the *NDPA's* automated decision-making safeguards. Across both, vendor accountability at the procurement stage offers the most concrete lever for translating constitutional principles into operational constraints. Source-code escrow and enforceable audit rights are what make that lever work.

Bibliography

Literature

Adeola and Mutua *Palgrave Handbook of Democracy*

Adeola A and Mutua M (eds) *The Palgrave Handbook of Democracy, Governance and Justice in Africa* (Palgrave Macmillan London 2022)

Brown and Marsden *Regulating Code*

Brown I and Marsden CT *Regulating Code: Good Governance and Better Regulation in the Information Age* (MIT Press Cambridge MA 2013)

<https://doi.org/10.7551/mitpress/8879.001.0001>

Cayford, Pieters and Van Gelder 2019 *Journal of Information, Communication and Ethics in Society*

Cayford M, Pieters W and Van Gelder PHAJM "Wanting It All – Public Perceptions of the Effectiveness, Cost, and Privacy of Surveillance Technology" 2019 *Journal of Information, Communication and Ethics in Society* 10-27 <https://doi.org/10.1108/JICES-11-2018-0087>

Chesterman 2021 *AJCL*

Chesterman S "Through a Glass, Darkly: Artificial Intelligence and the Problem of Opacity" 2021 *AJCL* 271-294

<https://doi.org/10.1093/ajcl/avab012>

Couldry and Mejias 2019 *Internet Policy Review*

Couldry N and Mejias U "Making Data Colonialism Liveable: How Might Data's Social Order Be Regulated" 2019 *Internet Policy Review* 1-20
<https://doi.org/10.14763/2019.2.1411>

Couldry and Mejias 2019 *Television & News Media*

Couldry N and Mejias U "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject" 2019 *Television & News Media* 336-349
<https://doi.org/10.1177/1527476418796632>

Daigle 2021 *Journal of International Commerce and Economics*

Daigle B "Data Protection Laws in Africa: A Pan-African Survey and Noted Trends" 2021 *Journal of International Commerce and Economics* 1-27

De Gregorio and Dunn 2022 *CMLR*

De Gregorio G and Dunn P "The European Risk-based Approaches: Connecting Constitutional Dots in the Digital Age" 2022 *CMLR* 473-500

De Gregorio and Radu 2022 *IJLIT*

De Gregorio G and Radu R "Digital Constitutionalism in the New Era of Internet Governance" 2022 *IJLIT* 68-87 <https://doi.org/10.1093/ijlit/eaac004>

De Hert and Gutwirth 2006 *CLSR*

De Hert P and Gutwirth S "Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the State" 2006 *CLSR* 61-104

Eubanks *Automating Inequality*

Eubanks V *Automating Inequality: How High-tech Tools Profile, Police, and Punish the Poor* (St Martin's Press New York 2018)

Feldstein *Rise of Digital Repression*

Feldstein S *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (Oxford University Press Oxford 2021)
<https://doi.org/10.1093/oso/9780190057497.001.0001>

Feldstein "Surveillance in the Illiberal State"

Feldstein S "Surveillance in the Illiberal State" in Sajó A, Uitz R and Holmes S (eds) *Routledge Handbook of Illiberalism* (Routledge New York 2021) 351-364

Foucault *Discipline and Punish*

Foucault M *Discipline and Punish: The Birth of the Prison* (Vintage Vancouver 1977)

Garner *Black's Law Dictionary*

Garner BA (ed) *Black's Law Dictionary* 12th edn (Thomson Reuters St Paul MN 2024)

Herold et al 2023 *International Journal of Physical Distribution and Logistics Management*

Herold S et al "Dynamic Capabilities for Digital Procurement Transformation: A Systematic Literature Review" 2023 *International Journal of Physical Distribution and Logistics Management* 424-447 <https://doi.org/10.1108/IJPDLM-12-2021-0535>

Jili 2022 *Nature*

Jili B "Africa: Regulate Surveillance Technologies and Personal Data" 2022 *Nature* 445-448 <https://doi.org/10.1038/d41586-022-01949-9>

Joneidy, Rahimian and Arciszewski 2024 *Law and Business*

Joneidy S, Rahimian F and Arciszewski T "Closing the Legal-Technical Gap in Digital Trade" 2024 *Law and Business* 1-15 <https://doi.org/10.2478/law-2024-0001>

Judge, Nitzberg and Russell 2025 *Policy and Society*

Judge B, Nitzberg M and Russell S "When Code isn't Law: Rethinking Regulation for Artificial Intelligence" 2025 *Policy and Society* 85-97 <https://doi.org/10.1093/polsoc/puae020>

Kademeteme and Bvuma 2023 *Journal of the British Blockchain Association*

Kademeteme E and Bvuma S "Using Blockchain Technology to Improve the Integrity and Transparency of Procurement Processes Between SMMEs and Government: A Systematic Literature Review" 2023 *Journal of the British Blockchain Association* 1-12 [https://doi.org/10.31585/jbba-7-1-\(1\)2024](https://doi.org/10.31585/jbba-7-1-(1)2024)

Lungu 2022 *American Journal of Qualitative Research*

Lungu M "The Coding Manual for Qualitative Researchers" 2022 *American Journal of Qualitative Research* 232-237 <https://doi.org/10.29333/ajqr/12085>

Lungu "Enhancing Public Service Delivery"

Lungu M "Enhancing Public Service Delivery in Government Procurement: A Review Exploring the Role of Artificial Intelligence and Automative Structures" in Reddick CG and Demir T (eds) *Handbook of Public Service Delivery* (2024) 188-204 <https://doi.org/10.4337/9781035315314.00019>

Lungu and McCue 2024 *Journal of AI Law and Regulation*

Lungu M and McCue C "Evaluating Regulatory Structures for the Expansion of Artificial Intelligence: A Systematic Review of US State Legislation" 2024 *Journal of AI Law and Regulation* 310-330 <https://doi.org/10.21552/aire/2024/3/7>

Maepa, Mpwanya and Phume 2023 *Journal of Transport and Supply Chain Management*

Maepa DN, Mpwanya MF and Phume TB "Readiness Factors Affecting E-procurement in South African Government Departments" 2023 *Journal of Transport and Supply Chain Management*
<https://doi.org/10.4102/jtscm.v17i0.874>

Martínez-Béjar and Brändle 2018 *Technology in Society*

Martínez-Béjar R and Brändle G "Contemporary Technology Management Practices for Facilitating Social Regulation and Surveillance" 2018 *Technology in Society* 139-148
<https://doi.org/10.1016/j.techsoc.2018.04.003>

Mittelstadt *et al* 2016 *Big Data & Society*

Mittelstadt BD *et al* "The Ethics of Algorithms: Mapping the Debate" 2016 *Big Data & Society* <https://doi.org/10.1177/2053951716679679>

Monahan 2008 *Surveillance & Society*

Monahan T "Surveillance and Inequality" 2008 *Surveillance & Society* 217-226 <https://doi.org/10.24908/ss.v5i3.3421>

Nandy 2023 *Journal of Current Social and Political Issues*

Nandy D "Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns" 2023 *Journal of Current Social and Political Issues* 13-17 <https://dx.doi.org/10.15575/jcspi.v1i1.442>

Nwafor 2021 *IJLIT*

Nwafor IE "AI Ethical Bias: A Case for AI Vigilantism (Ailantism) in Shaping the Regulation of AI" 2021 *IJLIT* 225-240
<https://doi.org/10.1093/ijlit/eaab008>

Nwafor 2023 *South African Intellectual Property Law Journal*

Nwafor IE "Artificial Intelligence Facial Recognition Surveillance and the Breach of Privacy Rights: The 'Clearview AI' and 'Rite Aid' Case Studies" 2023 *South African Intellectual Property Law Journal* 88-92
<https://doi.org/10.47348/SAIPL/v11/a5>

Nwafor 2024 *AJLS*

Nwafor IE "Cybercrime Investigation and Prosecution in Nigeria: Bridging the Gaps" 2024 *AJLS* 249-270 <https://doi.org/10.1163/17087384-12340108>

Nyabola "Africa's Digital Public Sphere"

Nyabola N "Africa's Digital Public Sphere" in Okeja U (ed) *Routledge Handbook of African Political Philosophy* (Routledge London 2023) 315-329

Panya and Awuor 2023 *Strategic Journal of Business & Change Management*

Panya KO and Awuor E "Public Procurement Reforms in Africa: Challenges, Constraints and Improvement Opportunities" 2023 *Strategic Journal of Business & Change Management* 1435-1456

Pasquale *Black Box Society*

Pasquale F *The Black Box Society: The Secret Algorithms that Control Money and Information* (Harvard University Press Cambridge MA 2015)

Sheombar and Skelton "Who Supplies Digital Surveillance Technologies?"

Sheombar A and Skelton SK "Who Supplies Digital Surveillance Technologies to African Governments?" in Roberts T and Mare A (eds) *Digital Surveillance in Africa: Power, Agency and Rights* (Zed Books London 2025) 183-210

Stevens *et al* 2023 *Big Data & Society*

Stevens A *et al* "'I Started Seeing Shadows Everywhere': The Diverse Chilling Effects of Surveillance in Zimbabwe" 2023 *Big Data & Society* <https://doi.org/10.1177/20539517231158631>

Roberts *et al* *Mapping the Supply of Surveillance Technologies to Africa*

Roberts T *et al* *Mapping the Supply of Surveillance Technologies to Africa: Case Studies from Nigeria, Ghana, Morocco, Malawi and Zambia* (Institute of Development Studies Brighton 2023) <https://doi.org/10.19088/IDS.2023.027>

Sule, Zennaro and Thomas 2021 *Technology in Society*

Sule MJ, Zennaro M and Thomas G "Cybersecurity Through the Lens of Digital Identity and Data Protection: Issues and Trends" 2021 *Technology in Society* <https://doi.org/10.1016/j.techsoc.2021.101734>

Taylor 2002 *Surveillance & Society*

Taylor N "State Surveillance and the Right to Privacy" 2002 *Surveillance & Society* 66-85 <https://doi.org/10.24908/ss.v1i1.3394>

Viljoen *International Human Rights Law*

Viljoen F *International Human Rights Law in Africa* 3rd edn (Oxford University Press Oxford 2022)

Wachter, Mittelstadt and Russell 2017 *Harv J L & Tech*

Wachter S, Mittelstadt B and Russell C "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR" 2017 *Harv J L & Tech* 841-887 <https://doi.org/10.48550/arXiv.1711.00399>

Zuboff *Age of Surveillance Capitalism*

Zuboff S *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs New York 2019)

Case law

AmaBhungane Centre for Investigative Journalism NPC v Minister of Justice and Correctional Services; Minister of Police v AmaBhungane Centre for Investigative Journalism NPC 2021 3 SA 246 (CC)

Vumacam (Pty) Ltd v Johannesburg Roads Agency (14867/20) [2020] ZAGPJHC 186 (20 August 2020)

Legislation**Egypt**

Penal Code No 58 of 1937

Telecommunications Regulation Law No 10 of 2003

Europe

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1

Kenya

Data Protection Act, 2019

Nigeria

Constitution of the Federal Republic of Nigeria, 1999

Cybercrimes (Prohibition, Prevention, etc) Act, 2015

Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act, 2024

Enforcement Process Regulations, 2019

Lawful Interception of Communications Regulations, 2019

Nigeria Data Protection Act, 2023

Nigeria Data Protection Regulation, 2019

Nigerian Communications Act, 2003

Rwanda

Constitution of Rwanda, 2003

South Africa

Constitution of the Republic of South Africa, 1996

Criminal Procedure Act 51 of 1977

Protection of Personal Information Act 4 of 2013

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

United States of America

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 115 Stat 272 (2001) (US Patriot Act)

Government publications

South Africa

Gen N 2533 in GG 50741 of 31 May 2024 (National Policy on Data and Cloud)

Regulation of Interception of Communications and Provision of Communication-Related Information Amendment Bill, 2023

International instruments

ACHPR Declaration of Principles on Freedom of Expression and Access to Information in Africa (2019)

ACHPR Resolution on the Right to Freedom of Expression and Access to Information on the Internet in Africa AU Doc ACHPR/Res362(LIX) (2016)

African Charter on Human and Peoples' Rights (1981)

AU Convention on Cyber Security and Personal Data Protection (2014) (Malabo Convention)

International Covenant on Civil and Political Rights (1966)

Internet sources

Access Now 2024 <https://www.accessnow.org/surveillance/>

Access Now 2024 *Standing Up to Surveillance* <https://www.accessnow.org/surveillance/> accessed 12 August 2025

Access Now 2024 <https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf>

Access Now 2024 *Internet Shutdowns in 2023: Shrinking Democracy, Growing Violence* <https://www.accessnow.org/wp-content/uploads/2024/05/2023-KIO-Report.pdf> accessed 15 June 2025

Access Now 2025 <https://www.accessnow.org/press-release/africa-keepiton-internet-shutdowns-2024/>

Access Now 2025 *A Blow to Human Rights in Africa: Internet Shutdowns in 2024* <https://www.accessnow.org/press-release/africa-keepiton-internet-shutdowns-2024/> accessed 1 June 2025

Access Now 2025 https://media.licdn.com/dms/document/media/v2/D4E1FAQHO-28C-2Wxlw/feedshare-document-pdf-analyzed/B4EZjNIFNxHoAc-/0/1755795712763?e=1767830400&v=beta&t=U3oaVP0wHzM7zlevRgaRwAryb_YT5BbF25j7ZRaEpGQ&acrobatPromotionSource=linkedin_chrome-post_view

Access Now 2025 *How Weak Data Protection Laws Enable Rights-abusing Surveillance Practices* Africa https://media.licdn.com/dms/document/media/v2/D4E1FAQHO-28C-2Wxlw/feedshare-document-pdf-analyzed/B4EZjNIFNxHoAc-/0/1755795712763?e=1767830400&v=beta&t=U3oaVP0wHzM7zlevRgaRwAryb_YT5BbF25j7ZRaEpGQ&acrobatPromotionSource=linkedin_chrome-post_view accessed 31 December 2025

Ademuyiwa and Adeniran 2020 https://www.cigionline.org/sites/default/files/documents/no244_0.pdf
Ademuyiwa I and Adeniran A 2020 *Assessing Digitalization and Data Governance Issues in Africa. CIGI Papers No 244* https://www.cigionline.org/sites/default/files/documents/no244_0.pdf accessed 10 May 2026

Al Jazeera 2020 <https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report>
Al Jazeera 2020 *Nigerian Intelligence Bought Tool to Spy on Citizens: Report* <https://www.aljazeera.com/news/2020/12/8/nigerias-defence-agency-acquires-spy-equipment-says-report> accessed 5 September 2025

Amnesty International 2021 <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>
Amnesty International 2021 *Forensic Methodology Report: How to Catch NSO Group's Pegasus* <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/> accessed 3 September 2025

AU 2022 <https://au.int/en/documents/20220728/au-data-policy-framework>
African Union 2022 *AU Data Policy Framework* <https://au.int/en/documents/20220728/au-data-policy-framework> accessed 11 May 2026

Brouwers 2024 <https://www.moneyweb.co.za/news/companies-and-deals/vumacam-announces-crime-fighting-partnership-with-gauteng-government/>

Brouwers T 2024 *Vumacam Announces Crime-fighting Partnership with Gauteng Government* <https://www.moneyweb.co.za/news/companies-and-deals/vumacam-announces-crime-fighting-partnership-with-gauteng-government/> accessed 3 September 2025

Federal Ministry of Communications and Digital Economy 2021 <https://nitda.gov.ng/wp-content/uploads/2021/05/REVISED-NATIONAL-DIGITAL-IDENTITY-POLICY-ON-SIM.pdf>

Federal Ministry of Communications and Digital Economy, Nigeria 2021 *Revised National Identity Policy for SIM Card Registration* <https://nitda.gov.ng/wp-content/uploads/2021/05/REVISED-NATIONAL-DIGITAL-IDENTITY-POLICY-ON-SIM.pdf> accessed 11 May 2026

First Distribution date unknown <https://firstdistribution.com/our-brands/isentry/>

First Distribution date unknown *iSentry* <https://firstdistribution.com/our-brands/isentry/> accessed 1 September 2025

Hao and Swart 2022 <https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid>

Hao K and Swart H 2022 *South Africa's Private Surveillance Machine is Fuelling a Digital Apartheid* <https://www.technologyreview.com/2022/04/19/1049996/south-africa-ai-surveillance-digital-apartheid> accessed 11 May 2026

Haritwal 2025 <https://www.nextmsc.com/report/africa-ai-cctv-market>

Haritwal S 2025 *Africa AI CCTV Market* <https://www.nextmsc.com/report/africa-ai-cctv-market> accessed 11 May 2026

Heywood and Pongweni 2023 <https://www.dailymaverick.co.za/article/2023-08-29-gauteng-crime-prevention-wardens-set-up-unlawfully-experts/>

Heywood M and Pongweni T 2023 *Gauteng's Crime Prevention Wardens were Set Up Unlawfully, Risk Abuse of Police Powers – Experts* <https://www.dailymaverick.co.za/article/2023-08-29-gauteng-crime-prevention-wardens-set-up-unlawfully-experts/> accessed 12 May 2026

Hillman and McCalpin 2019 <https://www.csis.org/analysis/watching-huaweis-safe-cities>

Hillman JE and McCalpin M 2019 *Watching Huawei's "Safe Cities"* <https://www.csis.org/analysis/watching-huaweis-safe-cities> accessed 12 May 2026

Human Rights Watch 2014 <https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia>

Human Rights Watch 2014 *"They Know Everything We Do": Telecom and Internet Surveillance in Ethiopia*

<https://www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia> accessed 12 May 2026

Human Rights Watch 2021

<https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses>

Human Rights Watch 2021 *Unchecked Spyware Industry Enables Abuses: Governments Should Halt Trade in Surveillance Technology*

<https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses> accessed 11 May 2026

INTERPOL 2025 <https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa>

INTERPOL 2025 *New INTERPOL Report Warns of Sharp Rise in Cybercrime in Africa*

<https://www.interpol.int/News-and-Events/News/2025/New-INTERPOL-report-warns-of-sharp-rise-in-cybercrime-in-Africa> accessed 11 May 2026

Kwet 2022 <https://saiia.org.za/research/the-city-surveillance-state-inside-johannesburgs-safe-city-initiative/>

Kwet M 2022 *The City Surveillance State: Inside Johannesburg's Safe City Initiative*

<https://saiia.org.za/research/the-city-surveillance-state-inside-johannesburgs-safe-city-initiative/> accessed 12 May 2026

Langa 2024 <https://www.theafricareport.com/354469/rise-of-chinese-surveillance-tech-in-africa-development-or-espionage/>

Langa V 2024 *Rise of Chinese Surveillance Tech in Africa: Development or Espionage?*

<https://www.theafricareport.com/354469/rise-of-chinese-surveillance-tech-in-africa-development-or-espionage/> accessed 11 May 2026

Mokwena 2024 <https://briefly.co.za/southafrica/180039-gauteng-premier-panyaza-lesufi-launches-7000-facial-recognition-cameras/>

Mokwena T 2024 *Gauteng Premier Panyaza Lesufi Launches Almost 7000 Facial Recognition Cameras*

<https://briefly.co.za/southafrica/180039-gauteng-premier-panyaza-lesufi-launches-7000-facial-recognition-cameras/> accessed 12 May 2026

MSN 2025 <https://www.msn.com/en-xl/africa/nigeria/huawei-cloud-showcases-ai-potential-at-lagos-forum/ar-AA1KJd0x\>

MSN 2025 *Huawei Cloud Showcases AI Potential at Lagos Forum* <https://www.msn.com/en-xl/africa/nigeria/huawei-cloud-showcases-ai-potential-at-lagos-forum/ar-AA1KJd0x\> accessed 12 May 2026

Nash 2022 <https://www.biometricupdate.com/202204/a-2020-court-fight-in-south-africa-reveals-dominance-of-biometric-surveillance-industry>

Nash J 2022 *A 2020 Court Fight in South Africa Reveals Dominance of Biometric Surveillance Industry*

<https://www.biometricupdate.com/202204/a-2020-court-fight-in-south-africa-reveals-dominance-of-biometric-surveillance-industry> accessed 12 May 2026

Privacy International 2018

<https://privacyinternational.org/explainer/2222/imsi-catchers>

Privacy International 2018 *IMSI Catchers*

<https://privacyinternational.org/explainer/2222/imsi-catchers> accessed 11 May 2026

Privacy International 2023

<https://privacyinternational.org/examples/5291/report-finds-african-countries-adopt-digital-surveillance-despite-human-rights-threat>

Privacy International 2023 *Report Finds African Countries Adopt Digital Surveillance Despite Human Rights Threat*

<https://privacyinternational.org/examples/5291/report-finds-african-countries-adopt-digital-surveillance-despite-human-rights-threat> accessed 11 May 2026

Roberts 2025 <https://www.ids.ac.uk/publications/understanding-digital-rights-definitions-conceptions-and-myths/>

Roberts T 2025 *Understanding Digital Rights: Definitions, Conceptions, and Myths* <https://www.ids.ac.uk/publications/understanding-digital-rights-definitions-conceptions-and-myths/>

accessed 1 September 2025

Roberts et al 2021 <https://www.ids.ac.uk/projects/surveillance-legislation-in-africa/>

Roberts T et al 2021 *Surveillance Law in Africa: A Review of Six Countries* <https://www.ids.ac.uk/projects/surveillance-legislation-in-africa/> accessed 24 July 2025

Robinson 2023 <https://www.ids.ac.uk/news/african-nations-spending-1bn-a-year-on-harmful-surveillance-of-citizens/>

Robinson S 2023 *African Nations Spending \$1bn a Year on Harmful Surveillance* <https://www.ids.ac.uk/news/african-nations-spending-1bn-a-year-on-harmful-surveillance-of-citizens/> accessed 11 May 2026

Sizwe Africa 2023 <https://www.itweb.co.za/article/digital-transformation-facial-recognition-technologies-anticipated-to-grow-despite-slowng-economic-growth/KWEBbvyLKPyqmRjO>

Sizwe Africa IT Group 2023 *Digital Transformation, Facial Recognition Technologies Anticipated to Grow Despite Slowing Economic Growth* <https://www.itweb.co.za/article/digital-transformation-facial-recognition-technologies-anticipated-to-grow-despite-slowng-economic-growth/KWEBbvyLKPyqmRjO> accessed 11 May 2026

Swart 2023 https://intelwatch.org.za/wp-content/uploads/2023/05/Intelwatch_Supplementary_report_Reforming_surveillance_in_South_Africa_May_2023.pdf

Swart H 2023 *Reforming Communication Surveillance in South Africa: Understanding the Section 205 "Loophole"* https://intelwatch.org.za/wp-content/uploads/2023/05/Intelwatch_Supplementary_report_Reforming_surveillance_in_South_Africa_May_2023.pdf accessed 12 May 2026

The Presidency 2024 <https://www.thepresidency.gov.za/president-ramaphosa-refers-rica-amendment-bill-national-assembly>

The Presidency, South Africa 2024 *President Ramaphosa Refers RICA Amendment Bill to National Assembly* <https://www.thepresidency.gov.za/president-ramaphosa-refers-rica-amendment-bill-national-assembly> accessed 12 May 2026

UNCTAD 2024 <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

United Nations Conference on Trade and Development 2024 *Data Protection and Privacy Legislation Worldwide* <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide> accessed 11 May 2026

World Bank 2021 <https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0>

World Bank 2021 *Mutual Recognition of IDs Across Borders* <https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0> accessed 11 May 2026

List of Abbreviations

ACHPR	African Commission on Human and Peoples' Rights
AI	artificial intelligence
AJCL	American Journal of Comparative Law
AJLS	African Journal of Legal Studies
AU	African Union
CCTV	closed-circuit television
CERT	Computer Emergency Response Team

CLSR	Computer Law and Security Review
CMLR	Common Market Law Review
GDPR	General Data Protection Regulation
Harv J L & Tech	Harvard Journal of Law and Technology
IJLIT	International Journal of Law and Information Technology
IMSI	International Mobile Subscriber Identity
NDPA	Nigeria Data Protection Act, 2023
POPIA	Protection of Personal Information Act 4 of 2013
RICA	Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002
SOC	Security Operations Centre
UK	United Kingdom
UNCTAD	United Nations Conference on Trade and Development
US	United States of America