IP AND DATA RIGHTS IN AFRICA'S DIGITAL ECONOMY: A PROTECTIVE–ADAPTIVE BLUEPRINT

Tanaka Dakacha*
Research and Teaching Associate, University of the Witwatersrand, School of Law

ABSTRACT

The rapid evolution of digital technologies is transforming Africa's economic landscape, reshaping how creative works are produced, distributed, and consumed. This shift presents both opportunities and challenges for intellectual property (IP) protection. Using South Africa, Kenya, and Nigeria as case studies, this paper explores the role of robust IP frameworks in fostering innovation, creativity, and sustainable growth in Africa's digital economy. It highlights how strong IP protection attracts technological investment and addresses issues such as digital piracy, copyright infringement, and rapid technological advancements. The paper also proposes strategies for harmonising IP laws across African jurisdictions, vital for regional integration under the African Continental Free Trade Area (AfCFTA).

It further examines data rights protection on digital platforms, focusing on ownership, consent, and the distribution of value. The paper discusses data ownership controversies and the need for regulatory harmonisation. By analysing the intersection of IP law, data rights, and digital innovation, it calls for adaptive policies that balance protection with access. Drawing from evolving IP regimes and AfCFTA protocols, it offers policy recommendations aligned with Agenda 2063 and global treaties. The comparative focus offers scalable insights, demonstrating how tailored reforms can enhance the creative industries, facilitate data flows, and attract investment — essential for equitable digital transformation and economic sustainability.

KEYWORDS: Intellectual property, data rights, digital economy, innovation, AfCFTA, legal frameworks

1. Introduction

Technologies like the Internet of Things and big data analytics could boost Africa's Gross Domestic Product (GDP) by up to $1.5 trillion by 2030, driving productivity and efficiency across industries.[1] Realising this potential depends on the development of legal frameworks that both protect and facilitate the circulation of digital assets. At present, intellectual property (IP) and data governance laws across African countries are highly fragmented. More than 50 national IP laws exist, alongside two regional organisations with overlapping mandates, namely the African Regional Intellectual Property

* BA LLB (University of the Witwatersrand) PGDip (University of the Witwatersrand) LLM (University of the Witwatersrand). Email: tanaka.dakacha@wits.ac.za

1 UNECA 'Artificial intelligence in African economic development potential and challenges to overcome', available at: https://repository.uneca.org/server/api/core/bitstreams/007111a4-d9d0-42ca-94c2-4f39a3ff044d/content (viewed on 21 July 2025).

https://doi.org/10.47348/SAIPL/v13/i2a12

Organization (ARIPO) and the African Intellectual Property Organization (OAPI). In addition, 32 separate data protection laws currently coexist,[2] with a continental treaty on cybersecurity, electronic transactions, and personal data protection, which remains unratified.[3] The Business Software Alliance, a Global Software Survey, shows that unlicensed software rates remain high in Africa, with 74% in Kenya, 80% in Nigeria, 89% in Zimbabwe, and 82% in Algeria, highlighting weak licensing compliance across the region.[4] This complex and inconsistent regulatory landscape increases compliance costs, discourages foreign investment, and limits Africa's ability to harness its rich cultural heritage and vast data resources.

Most existing statutes governing IP and data regulation in African countries were formulated during the analogue era,[5] prior to the emergence of platform economies, cloud computing, and algorithmic data extraction. As a result, they are ill-equipped to address the complexities of the digital age. Key legal and policy questions remain unresolved, including who owns non-personal, machine-generated data in African markets, how innovators can secure enforceable intellectual property rights (IPR) without entrenching knowledge monopolies, and whether the African Continental Free Trade Area's (AfCFTA) new protocols can achieve the regulatory coherence still lacking in ARIPO and OAPI. Without clear, harmonised legal frameworks, Africa risks exporting raw data while importing costly digital services, limiting its full participation in the global digital economy.

This article argues that Africa's digital transformation is unlikely to progress meaningfully unless IP and data-rights laws evolve to be both protective and adaptive. Protective frameworks are essential to reward creativity and attract investment, while adaptive mechanisms are necessary to ensure equitable access, promote open science, and generate developmental spillovers. The article proposes a calibrated, Afro-centric model grounded in key continental and international instruments, including the AfCFTA Protocol on Intellectual Property Rights (IP Protocol), the AfCFTA Digital Trade Protocol (Digital Trade Protocol), the Malabo Convention, Agenda 2063, and selected global benchmarks. This paper examines how African jurisdictions can modernise IP and data-governance frameworks without replicating colonial or extractive logics, while balancing protection and access to foster innovation, equitable value distribution, and public-interest research. It also examines how AfCFTA's emerging digital architecture can enable a harmonised, context-sensitive model across the continent. Methodologically, it combines doctrinal

2 AU 'Data policy framework', available at: https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf (viewed on 21 July 2025).

3 AU 'African Union convention on cyber security and personal data protection', available at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (viewed on 21 July 2025).

4 BSA 'Global software survey', available at: https://gss.bsa.org/wp-content/uploads/2018/05/2018_BSA_GSS_Report_en.pdf (viewed on 21 July 2025).

5 J de Beer J Baarbé & CB Ncube 'Evolution of Africa's Intellectual property treaty ratification landscape' (2018) 22 *The African Journal of Information and Communication* 60.

https://doi.org/10.47348/SAIPL/v13/i2a12

analysis of South African law (including the Protection of Personal Information Act, the Copyright Act, and the Competition Act), comparative insights from Kenya, Nigeria, the European Union (EU), the United States (US), and Brazil, and a treaty-text analysis of AfCFTA instruments, distinguishing descriptive mapping from normative proposals.

To address these questions, the paper proposes a protective–adaptive blueprint built around four regulatory 'dials' covering patents and compulsory licensing, copyright and text-and-data mining, trade secrets and secure Application Programming Interface (API) access, and database rights with open licences. These dials operate as flexible mechanisms that can be adjusted based on evidence, market conditions, and public-interest needs. The paper combines doctrinal analysis, comparative insights from African and global jurisdictions, treaty-text interpretation, and a political economy perspective, culminating in an operational design for the dials, the role of regulatory sandboxes under AfCFTA, and institutional mechanisms for AI governance and implementation, before concluding with broader regional and developmental implications.

2. Case Study Selection

Africa's digital economy governance cannot be understood or reformed through abstract continental averages. This paper therefore focuses its empirical inquiry mostly on South Africa, Kenya, and Nigeria. These countries offer a high-impact, regionally balanced, and legally diverse foundation for testing the protective and adaptive thesis introduced in this paper. The World Bank reports that Nigeria, South Africa, and Kenya account for over half of sub-Saharan Africa's GDP, and Partech indicates they attract 68–74% of the continent's venture capital.[6] Each country hosts a prominent innovation hub, including Cape Town's financial technology corridor, Nairobi's Silicon Savannah, and Lagos's Yabacon Valley, making them ideal environments for regulatory experimentation. From a legal standpoint, they represent a broad spectrum of approaches. South Africa maintains IP statutes from the mid-twentieth century, supported by specialised courts. Kenya's Copyright (Amendment) Act 2022 modernised copyright administration and rights management, but text-and-data mining (TDM), remains governed by fair dealing, especially for scientific research, without a specific statutory exception. Nigeria combines a localisation-oriented Data Protection Regulation with the continent's largest untapped consumer market. None of these countries is a member of ARIPO or OAPI, which highlights the transaction cost barriers that the AfCFTA protocols aim to address. The outcomes of digital governance reforms in these jurisdictions will provide valuable policy insights for other African states, both within and outside the regional IP offices.

6 Partech Africa '2024 Africa venture capital', available at: https://partechpartners.com/africa-reports/2024-africa-tech-venture-capital-report (viewed on 21 July 2025).

https://doi.org/10.47348/SAIPL/v13/i2a12

2.1 Constitutional framework

South Africa anchors the paper's protective adaptive blueprint through its constitutional framework and hybrid common-law and statutory mechanisms in IP, data protection, and competition law. South Africa's constitutional framework provides the foundation for interpreting IP, data, and competition laws, with four key provisions shaping digital governance. Section 14 of the Constitution protects against unlawful collection and use of personal data,[7] forming the basis for the Protection of Personal Information Act, 2013 (POPIA) mandate of lawful, minimal, and proportionate processing.[8] This is the constitutional foundation for restricting intrusive data collection, algorithmic surveillance, and indiscriminate scraping for AI training. Section 16(1)*(a)* protects the freedom to receive and impart information,[9] a principle central to debates on TDM, reverse engineering, and research exceptions. Copyright limits reproduction, but expression rights require a narrow interpretation of these limits when they hinder research, information access, or academic inquiry.

Additionally, IP is treated as property under s 25,[10] but the right is limited by justifiable restrictions under s 36. This is relevant when balancing exclusive rights against public-interest tools like compulsory licensing, TDM exceptions, and mandated data access in competition cases. The right to access state-held information underpins open-data initiatives and data-sharing duties, especially for publicly funded datasets with high social value. Section 32 provides constitutional grounding for open-data principles and data-sharing obligations, particularly concerning publicly funded datasets. Section 36 requires that any limitation of rights be lawful, reasonable, and justifiable.[11] This proportionality test is the key framework for reconciling copyright, privacy, competition, and data-protection interests in AI training and digital-market regulation.

3. Intellectual Property in the Digital Age

Digitalisation has profoundly transformed both the value and the vulnerability of intangible assets. Traditional copyright and patent doctrines, developed in the nineteenth century, were premised on the scarcity of physical copies and the existence of territorially bounded markets. The South African Copyright Act requires originality and fixation for copyright,[12] and prohibits unauthorised reproduction.[13] South African courts have refined these concepts through tests for originality (skill and labour), fixation, and substantial reproduction. In *Moneyweb (Pty) Ltd v Media 24 Ltd (Moneyweb)*, the court clarified that originality stems from the author's skill and judgment, fixation

7 Section 14 of the Constitution of the Republic of South Africa, 1996.
8 Section 2 of the Protection of Personal Information Act, 2013.
9 Section 16(1)*(a)* of the Constitution (n7).
10 Section 25 of the Constitution (n7).
11 Section 36 of the Constitution (n7).
12 Section 2(2) of the Copyright Act 98 of 1978.
13 Section 23 of the Copyright Act (n12).

https://doi.org/10.47348/SAIPL/v13/i2a12

from material embodiment, and infringement from reproducing a substantial part of the work.[14] In contrast, contemporary content production takes place within cloud-based environments, where replication is instantaneous and distribution is facilitated by algorithms. This doctrinal dissonance is illustrated in *Moneyweb*, a landmark South African case on online copyright. The High Court recognised that news articles published exclusively on a website could meet the statutory requirement of fixation, yet it faced challenges in assessing originality and substantial reproduction within a dynamic digital ecosystem.[15] The case exposes the disconnect between analogue legal categories and cloud-native content, emphasising the need for legal frameworks that reflect the technological realities of digital creation and distribution.

The court held that online news articles are fixed once stored in a database.[16] The decision affirmed that digital fixation holds the same legal status as physical fixation, guaranteeing copyright protection for works published online. The court applied the traditional 'sweat of the brow' doctrine, holding that originality demands a demonstrable degree of skill, effort, and labour in the work's creation.[17] Outputs generated purely through mechanical or automated processes lack originality unless there is clear evidence of human contribution. In assessing whether Media24 had infringed Moneyweb's rights, the court focused on the qualitative significance of the material used.[18] Copying short extracts may still be significant if they include the core elements of the original work. This is directly relevant to TDM. If machine learning models extract 'substantial' portions, even for non-expressive analysis, infringement may occur unless a statutory exception applies.

Despite the traditional four-part structure of IP, which remains formally intact, including copyright, patents, trademarks, and trade secrets, each component is undergoing significant reinterpretation in response to technological developments. Copyright law now routinely includes computer programs and structured databases.[19] Courts are increasingly faced with automatically generated texts and images that challenge established principles of authorial origin. Patent law is grappling with the unprecedented question of whether an artificial intelligence (AI) system can be recognised as an inventor, as illustrated by the DABUS filings submitted in South Africa and other jurisdictions.[20] South Africa's patent regime, governed by the Patents Act 57 of 1978,[21] uses a depository system that requires only formal examination, not substantive review for novelty or inventive step. The Companies and Intellectual Property

14 *Moneyweb (Pty) Limited v Media 24 Limited & another* 2016 3 SA 193 (GJ).
15 Ibid.
16 *Moneyweb* (n14) para 92.
17 *Moneyweb* (n14) paras 94–98.
18 *Moneyweb* (n14) paras 109–113.
19 WIPO *Intellectual Property Handbook* (2004) 43.
20 D Thaldar & M Naidoo 'AI inventorship: The right decision?' (2021) 117 *South African Journal of Science* at 2.
21 Sections 25–34 of the Patents Act 57 of 1978.

Commission (CIPC) performs no substantive evaluation of novelty, inventive step, or inventorship.[22] In July 2021, South Africa published a patent naming DABUS, an AI system, as the inventor.[23] This was not a judicial ruling but a procedural outcome, as the CIPC conducted only a formalities examination without substantive review.[24] No judicial precedent exists on whether an AI can qualify as an inventor under South African law, and the decision reflects administrative permissiveness rather than doctrinal acceptance.

Disclosure requirements are also under pressure due to the opaque nature of machine learning models. Trademark protection has expanded beyond physical labels to include domain names, hashtags, and assets within virtual environments,[25] which complicates the distinction between source identifiers and digital goods. Trade secret regimes, which were traditionally applied to manufacturing processes, are now being used to protect training datasets and neural network weights.[26] However, the emphasis on secrecy increasingly clashes with efforts to regulate algorithmic transparency, highlighting the need for legal frameworks that reflect the realities of digital innovation.

Digital convergence has thus created both overlaps and gaps within existing IP frameworks. A single mobile money application may be protected simultaneously by copyright for its source code, by patent law for its encryption algorithm, and by trade secret law for its fraud detection heuristics. This convergence raises complex questions about overlapping protections and the possibility of double enforcement. In contrast, raw non-personal datasets often fall outside the scope of traditional IP categories. As a result, many African start-ups rely exclusively on contractual agreements to prevent unauthorised use of their data. Empirical evidence suggests that gaps in legal coverage contribute to widespread software piracy in several AU member states.[27] Overlapping protections are often layered to deter competition, highlighting the need for coherent and balanced legal reform.

There is increasing agreement among scholars that IP regulation should adopt a layered and context-sensitive approach.[28] This model adjusts the strength of exclusive rights based on the societal value of openness, guided by sector-specific factors like responsiveness to research and public health benefits. This perspective aligns with AU's Digital Transformation Strategy, which advocates for knowledge assets that are strategically protected while remaining

22 Section 34 of the Patents Act (n21). South Africa uses a depository patent system, where the CIPC verifies applications only for formal compliance. See also Department of Trade and Industry 'Intellectual Property Policy of the Republic of South Africa Phase I', available at: https://www.gov.za/sites/default/files/gcis_document/201808/41870gen518_1.pdf (viewed 21 November 2025).

23 Thaldar & Naidoo (n20).

24 Ibid.

25 WIPO (n19) 234.

26 J Villasenor 'Artificial intelligence, trade secrets, and the challenge for transparency' (2024) 25 *North Carolina Journal of Law & Technology* 496.

27 Partech Africa (n6).

28 JA Ogbodo 'Beyond the 'spaghetti bowl': Assessing the role of the AfCFTA protocol on intellectual property in Africa's complex regulatory environment' (2024) 20 *Journal of Intellectual Property Law & Practice* 9.

https://doi.org/10.47348/SAIPL/v13/i2a12

oriented toward inclusive development, as envisioned in Agenda 2063.[29] In practice, this approach involves combining strong IP protections with mechanisms that promote access and equity. Examples include public interest compulsory licensing for patents, fair dealing and TDM exceptions for copyright, competition law-based data access orders for trade secrets, and Creative Commons licensing for publicly funded datasets.

3.1 Data rights and digital sovereignty

The legal status of raw, non-personal data remains one of the most unresolved issues in African IP law.[30] Unlike protected works or inventions, data types such as telemetry, coordinates, and sensor readings typically fall outside the scope of established IP laws. As a result, such data is often treated as *res nullius*, meaning a thing that belongs to no one,[31] unless it is contractually restricted. This doctrinal gap has drawn growing attention from policymakers, who increasingly invoke digital sovereignty.[32] Digital sovereignty refers to a political community's ability to define, enforce, and benefit from the rules governing data generated within its territory.[33] The AU's Data Policy Framework interprets sovereignty in explicitly developmental terms, linking control over data flows to industrial diversification and the ability to capture value across the digital value chain.[34] The concept of digital sovereignty underscores the need for Africa to control data generated within its borders, regulate cross-border data flows, set AI training rules, protect African languages and cultural archives, build local digital infrastructures, and strengthen public digital capacity.

Two primary regulatory models have taken shape in the governance of data across African jurisdictions. The first, illustrated by Nigeria's Data Protection Act, 2023 (NDPA) and Kenya's Data Protection Act, 2019 relies on data localisation requirements. In Nigeria, the NDPA restricts the cross-border transfer of personal data unless the destination country or transfer mechanism provides an adequate level of protection, or a specific exception applies under s 43 of the Act.[35] The NDPA establishes the Nigeria Data Protection Commission (NDPC) as a statutory regulator.[36] It introduces adequacy and transfer rules,[37] aligned with frameworks such as South Africa's POPIA and the Kenyan Data Protection Act. It incorporates sector-specific localisation

29 AU 'Digital transformation strategy for Africa (2020–2030)', available at: https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf (viewed on 21 July 2025).
30 M Hennemann 'African data protection laws and artificial intelligence – regulation, policy and ways forward' in LA Abdulrauf & H Dube (eds) *Data Privacy Law in Africa: Emerging Perspectives* (2024) 142.
31 D Thaldar 'The wisdom of claiming ownership of human genomic data: A cautionary tale for research institutions' (2020) 25 *Developing World Bioethics* 19.
32 M Santaniello 'Attributes of digital sovereignty: A conceptual framework' (2025) *Geopolitics* at 8.
33 Ibid.
34 Data Policy Framework (n2).
35 Section 41 of the Nigeria Data Protection Act, 2023.
36 Section 4 of the Nigeria Data Protection Act (n35).
37 Sections 41–42 of the Nigeria Data Protection Act (n35).

preferences for public-sector data,[38] and provides sanctions and enforcement mechanisms, although these remain limited by capacity constraints.[39]

Kenya's Data Protection Act provides for consent,[40] and legitimate-interest processing, localisation of critical personal data,[41] and registration and reporting duties for data controllers.[42] The Act similarly authorises the Cabinet Secretary to designate categories of data processing that, on grounds of the State's strategic interests or revenue protection, must be conducted through servers or data centres located within Kenya.[43] Supporters of localisation argue that it enhances cybersecurity, ensures the availability of evidence for domestic legal proceedings, and stimulates demand for local cloud infrastructure.[44] Opponents argue that mandatory localisation fragments the global internet, increases operational costs, especially for small and medium-sized enterprises (SMEs), and may be used to justify surveillance practices that undermine civil liberties.[45] Senegal's €70 million Huawei-built data centre in Diamniadio, hailed by President Sall as a milestone in digital sovereignty, also raises concerns about foreign technology dependence and geopolitical influence.[46] Kenya's localisation provisions highlight the tension between digital sovereignty and the Digital Trade Protocol, which discourages unjustified data localisation.[47]

The second model favours adequacy over strict data localisation. Article 20 of the AfCFTA Digital Trade Protocol proposes a unified authorisation system for cross-border data transfers.[48] This system, informally referred to by commentators as the 'African Passport', would be conditional on each participating country meeting baseline privacy and security standards to be specified in an annex.[49] The goal is to strike a balance between the economic benefits of data mobility and the need for consistent safeguards across jurisdictions. This continental passport model draws inspiration from, but does not replicate, the European Union's (EU) adequacy framework under the

38 Section 41 of the Nigeria Data Protection Act (n35).
39 Sections 46–53 of the Nigeria Data Protection Act (n35).
40 Section 30 of the Kenya Data Protection Act 24 of 2019.
41 Section 50 of the Kenya Data Protection Act (n40).
42 Sections 18–23 of the Kenya Data Protection Act (n40).
43 Section 50 of the Kenya Data Protection Act (n40).
44 A Mathew 'Cloud data sovereignty governance and risk implications of cross-border cloud storage', available at: https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage (viewed on 21 November 2025).
45 UNCTAD 'Digital economy report 2021', available at: https://unctad.org/system/files/official-document/der2021_en.pdf (viewed on 21 July 2025).
46 E Sine 'The Diamniadio datacenter, the driving force behind Senegal's digital transformation', available at: https://senegalnumeriquesa.sn/en/actualites/le-datacenter-de-diamniadio-lieu-d%E2%80%99impulsion-de-la-transformation-digitale-du-s%C3%A9n%C3%A9gal (viewed on 21 July 2025).
47 AU 'Protocol to the agreement establishing the African continental free trade area on digital trade' art 20, available at: https://au.int/en/treaties/protocol-agreement-establishing-african-continental-free-trade-area-digital-trade (viewed on 21 July 2025).
48 Ibid.
49 Ibid.

https://doi.org/10.47348/SAIPL/v13/i2a12

General Data Protection Regulation (GDPR).[50] By streamlining compliance, it aims to ease the regulatory burden on African firms navigating multiple, often conflicting export rules. The passport would function similarly to the EU's adequacy decision.[51] Once a state meets defined data-protection standards, it receives a continental 'passport,' enabling free data flows between passported states without separate compliance checks. This approach simplifies cross-border transfers, reduces regulatory fragmentation, and coexists with national laws, as domestic regulators retain oversight.

At a normative level, both localisation and adequacy raise issues of data ownership and control. Civil law systems treat data controllers as custodians with stewardship obligations rather than as proprietors, while common law jurisdictions rely on breach of confidence to curb misuse without conferring full ownership rights.[52] Some scholars advocate for a unique property right for high-investment datasets, echoing the EU's Database Directive, but others caution that such appropriation could create barriers to AI development and international research collaboration.[53] African regulators are increasingly using tiered data classification to tailor legal obligations. South Africa's POPIA distinguishes between personal, special personal, and de-identified data.[54] This framework supports differentiated regulation, imposing stricter rules on sensitive data like health or biometrics, and lighter ones on anonymised telemetry. This approach provides a more adaptable alternative to blanket data localisation mandates.

POPIA governs personal data processing in South Africa, balancing constitutional privacy rights with lawful use for business, research, and innovation.[55] Personal information relates to any identifiable person, special personal information covers sensitive data like children's, health, biometric, and belief details, while de-identified information cannot reasonably be linked to an individual.[56] Processing is lawful when based on consent, contractual necessity, legal obligation, legitimate interest, or public interest.[57] This provision is crucial for AI training as data controllers must justify processing personal information for model development. Additionally, cross-border transfers are permitted if the destination offers adequate protection, binding

50 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) (2016) art 45, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng (viewed on 21 November 2025).

51 Ibid. Under the EU GDPR, an adequacy decision is the European Commission's finding that a non-EU country provides data protection essentially equivalent to the EU's, allowing personal-data transfers without further safeguards.

52 AB Makulilo 'Data privacy in Africa: taking stock of its development after two decades' in LA Abdulrauf & H Dube (eds) *Data Privacy Law in Africa: Emerging Perspectives* (2024) 53.

53 V Tumalavičius et al 'Legal impacts of digitization on intellectual property' (2024) 13 *Amazonia Investiga* 219.

54 Section 1 of the Protection of Personal Information Act, 2013.

55 Section 9 of POPIA (n54).

56 Section 1 of POPIA (n54).

57 Section 4 of POPIA (n54).

agreements ensure equivalent safeguards, the data subject consents, or the transfer is necessary for a contract or public interest.[58]

However, digital sovereignty is closely linked to infrastructure and cannot be achieved through legal frameworks alone. Africa hosts only a small share of global data-centre capacity,[59] despite representing a significant portion of the world's population. Aspirations for sovereignty that rely solely on statutory provisions, without parallel investment in domestic server facilities and undersea cable redundancy, risk remaining symbolic. Recognising this, the AU's Digital Transformation Strategy combines normative governance with a concrete infrastructure plan.[60] It promotes the development of regional cloud zones and open-access fibre corridors to reduce costs while maintaining jurisdictional control over data flows.[61]

3.2 Intersections of IP and data governance

Digitisation blurs the line between proprietary knowledge and seemingly ownerless data streams. Modern digital platforms gain an edge by combining proprietary code and algorithms with massive streams of user and sensor data.[62] In most African jurisdictions, this data is not formally recognised as property. Competition economists describe this dynamic as a feedback flywheel.[63] Larger data pools improve algorithmic accuracy, which in turn attracts additional users, who contribute further data. The result is a self-reinforcing cycle of market concentration, raising familiar antitrust concerns in a new technological landscape.

Several competition authorities across Africa have begun treating control over large, unique datasets or platform interfaces as an 'essential facility', or at least a significant barrier to entry, when investigating digital market conduct and mergers.[64] The essential facilities doctrine asks whether a dominant firm controls a facility, whether that facility is indispensable for competition, whether rivals can practically or economically replicate it, and whether refusal to grant access is objectively justified.[65] Traditionally applied to physical infrastructure

58 Section 72 of POPIA (n54).

59 African Union 'The state of African digital infrastructure' (2025), available at: https://cms.d4dhub.eu/assets/Africa-Digital-Infrastructure-Report.pdf (viewed on 21 November 2025). Africa's limited data-centre capacity undermines digital sovereignty and AI development by forcing reliance on offshore infrastructure, which weakens local data control, increases compliance costs, and restricts the development of context-specific AI systems.

60 Digital Transformation Strategy (n29).

61 Ibid.

62 OECD 'Algorithms and collusion: competition policy in the digital age', available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2017/05/algorithms-and-collusion-competition-policy-in-the-digital-age_02371a73/258dcb14-en.pdf (viewed on 21 July 2025).

63 In competition economics, the 'feedback flywheel' describes a self-reinforcing cycle where user data improves algorithms, better services attract more users, and the growing user base generates even more data.

64 World Bank 'Competition policy in digital markets in Africa', available at: https://openknowledge.worldbank.org/server/api/core/bitstreams/ab6e84af-5512-44db-8f88-5548b02e40ae/content (viewed on 21 July 2025).

65 NI Moleya & T Shumba 'The conceptualisation of an essential facility: A comparative analysis of the positions in South Africa and the European Union' (2024) 38 *Speculum Juris Law Journal* 336.

https://doi.org/10.47348/SAIPL/v13/i2a12

like pipelines and ports, the doctrine now extends to digital assets, as courts and competition authorities increasingly view certain data and platforms as indispensable and irreproducible. South Africa's Competition Act already allows for a flexible interpretation of the essential facility concept in digital data contexts, with the GovChat case serving as a testing ground.[66] A facility is considered essential if access is indispensable, duplication is impractical or uneconomical, and refusal to supply would harm competition.[67] The doctrine applies when platforms control non-replicable datasets, proprietary APIs, or algorithmic infrastructures. This approach mirrors traditional obligations in network industries, such as sharing railway infrastructure or telecom interconnection points. However, it shifts the discussion into the realm of IP, as secure API designs and data-sharing protocols inevitably involve the exposure of trade secrets and database extraction rights.

In the digital economy, essential facilities may include non-replicable datasets, core platform APIs, mobile ecosystems, payment systems, cloud environments, and unique machine-learning resources. Whether these qualify depends on factual and economic analysis, but the principle remains that if a facility is indispensable and access denial forecloses competition, intervention may be warranted. In the GovChat case, the Competition Tribunal of South Africa found a *prima facie* case that Meta's refusal to let GovChat use its WhatsApp Business API amounted to exclusionary conduct,[68] highlighting the power of platform intermediaries, data-driven network effects, and the need for Fair, Reasonable, and Non-Discriminatory (FRAND), based API access. This case is significant because the Commission argued that the WhatsApp Business API may constitute an essential facility, marking a potential first recognition of digital essential facilities in South African law. It also reflects a broader shift toward platform accountability, with enforcement focusing on API access, gatekeeping, and algorithmic control, acknowledging that digital markets require proactive intervention. The referral further proposes FRAND access conditions, aligning South Africa with global regulatory trends such as the EU Digital Markets Act.

Additionally, data-rich machine learning models increasingly challenge the foundational principles of copyright and related rights. Deep learning systems trained on large collections of images or text now produce outputs such as synthetic voices, photographs, and written paragraphs that are new in form but derivative in origin.[69] These challenges reflect a broader policy dilemma regarding whether compulsory licensing and data sharing should be incorporated into IP law or addressed through competition and sector-specific

66 S Gumede & P Manenzhe 'Competition regulation for digital markets: The South African experience' (2023) 31 The *African Journal of Information and Communication* 14.

67 Moleya & Shumba (n65).

68 Competition Commission South Africa 'Facebook prosecuted for abusing its dominance' (2022), available at: https://www.compcom.co.za/wp-content/uploads/2022/03/FACEBOOK-PROSECUTED-FOR-ABUSING-ITS-DOMINANCE.pdf (viewed 21 November 2025).

69 WIPO 'Generative Artificial Intelligence: Patent Landscape Report (2024), available at: https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2007-en-generative-ai.pdf (viewed 21 November 2025).

regulation. The first approach risks weakening the exclusivity that supports investment in data curation and machine learning development. The second may struggle to provide legal certainty in advance, especially for start-ups that rely on predictable access to datasets for training initial algorithms. The AfCFTA Digital Trade Protocol points toward a hybrid solution by proposing an annex on Cross-Border Data Transfers.[70] This annex is expected to outline both privacy protections and market access conditions for data-driven services. If Africa adopts open and accountable data sharing, as the EU's Data Act, it could avoid the choice between treating data as property or as an unregulated common resource.

4. Sustainable Development and Agenda 2063

The AU's Agenda 2063, titled 'The Africa We Want', identifies the digital economy as a key driver of inclusive growth, cultural renewal, and gender equality.[71] Aspiration 1 commits to building a prosperous Africa rooted in inclusive growth and sustainable development.[72] Flagship Project 13, which addresses cybersecurity and the digital economy, urges Member States to establish IP and data governance frameworks tailored to African contexts.[73] The goal is to enable creative and knowledge-intensive sectors to move up the value chain. The policy rationale is clear. Without enforceable and context-sensitive IPR and interoperable data rules that respect rights, Africa's creative industries, fintech innovators, and AI start-ups risk remaining suppliers of raw talent and data, rather than becoming owners of high-value digital assets.

The AfCFTA's Phase II negotiations on IP, investment, and competition provide a concrete route for translating Agenda 2063's aspirational goals into enforceable trade law. The IP Protocol, adopted in February 2023, includes several provisions that embody this ambition.[74] These include special provisions for Least Developed Countries (LDCs),[75] technology transfer incentives modelled on Trade-Related Aspects of Intellectual Property Rights (TRIPS) art 66.2,[76] and *sui generis* protections for Traditional Knowledge and Genetic Resources with equitable benefit-sharing requirements.[77] This alignment reflects Aspiration 5 of Agenda 2063, which envisions an Africa rooted in a strong cultural identity and shared values.[78] The IP Protocol promotes development-oriented IP governance by ensuring the commercialisation of indigenous

70 Article 20 of the AU Digital Trade Protocol (n47).
71 AU 'Agenda 2063: The Africa we want', available at: https://au.int/sites/default/files/documents/36204-doc-agenda2063_popular_version_en.pdf (viewed on 21 July 2025).
72 Ibid.
73 AU 'Flagship Projects of Agenda 2063', available at: https://au.int/en/agenda2063/flagship-projects (viewed on 21 July 2025).
74 AU 'Protocol to the agreement establishing the African continental free trade area on intellectual property rights', available at: https://au.int/en/treaties/protocol-agreement-establishing-african-continental-free-trade-area-intellectual-property (viewed on 21 July 2025).
75 Article 35 of the AU Protocol (n74).
76 Ibid.
77 Ibid.
78 AU Agenda 2063 (n71).

https://doi.org/10.47348/SAIPL/v13/i2a12

cultural expressions benefits source communities, not just global entertainment firms. African innovation often arises through communal authorship, iterative adaptation, and oral transmission, as documented in Indigenous Knowledge systems.[79] Western IP structures, however, rest on individual authorship, fixation, exclusive ownership, limited transferable rights, and market-driven incentives. This mismatch systematically excludes African knowledge forms from formal IP protection.

Moreover, the Digital Trade Protocol adopted in February 2024 represents a significant step toward harmonising data governance across the continent. It includes a proposed annex on Cross-Border Data Transfers, informally referred to as the 'African Passport'.[80] The annex aims to consolidate fragmented national data transfer regimes within a continental framework, establishing shared data protection standards. This would advance Sustainable Development Goals (SDGs) 9 and 17 by easing compliance for SMEs and enhancing legal certainty for foreign investors. Aligned with the AU's Digital Transformation Strategy, which emphasises trusted data spaces as crucial to digital public goods, the AfCFTA's legal framework offers a practical tool for advancing Agenda 2063 through enforceable, scalable regulation.

Together, Agenda 2063, the AU's Digital Transformation Strategy, and the AfCFTA Phase II protocols form a policy triad that links strategic vision, sectoral planning, and legal implementation. Realising the framework's benefits depends on timely ratification, adequate enforcement resources, and a balanced approach to proprietary rights and openness. This balance is the central concern of this paper, which aims to theorise and implement a framework that supports both innovation and inclusivity. If these efforts fall short, African innovators may remain on the margins of global value chains. If successful, they will be positioned to lead a digital future that is inclusive, culturally rich, and economically diverse.

5. Mapping Africa's Existing IP and Data-Rights Landscape

Africa's legal framework for intangible assets reflects a patchwork of overlapping systems shaped more by historical legacy than deliberate design. At the continental level, two regional IP offices are responsible for administering registrable rights. ARIPO, headquartered in Harare and historically associated with former British colonies, comprises 22 member states.[81] OAPI, headquartered in Yaoundé and rooted in French civil law, serves seventeen francophone countries.[82] Collectively, these offices encompass not all of the AU's 55 member states and operate under distinct legal frameworks.

79 C Oguamanam *International Law and Indigenous Knowledge: Intellectual Property, Plant Biodiversity, and Traditional Medicine* (2006) 34.

80 Article 20 of the AU Digital Trade Protocol (n47).

81 ARIPO 'Member states', available at: https://www.aripo.org/member-states (viewed on 21 July 2025).

82 OAPI 'Member states', available at: https://oapi.int/en/presentation/member-states/ (viewed on 21 July 2025).

ARIPO functions through accession to international agreements, including the Harare Protocol on Patents and Designs (1984) and the Banjul Protocol on Trademarks (1993). By contrast, OAPI operates under a unitary system established by the Bangui Agreement, which was revised in 2015. As of April 2025, none of the four largest economies in Africa — South Africa, Egypt, Algeria, and Nigeria — is a member of either organisation.[83] This requires innovators to file in multiple national jurisdictions, raising administrative complexity and financial costs.

Below the continental tier, Africa's legal landscape comprises several Regional Economic Communities (RECs), including COMESA, Southern Africa Development Community (SADC), East African Communities (EAC) and Economic Communities of West African States (ECOWAS). These RECs have generally adopted soft law instruments rather than binding treaties. The absence of binding rules leads to continued legal fragmentation, as states selectively adopt provisions aligned with their national industrial policies. Legal diversity is even more evident at the national level. African states differ markedly in legal age, scope of rights, exceptions, treatment of traditional knowledge, data-transfer rules, and enforcement capacity. The contrasts among South Africa, Kenya, and Nigeria highlight the extent of this divergence and suggest that harmonisation should proceed through modular alignment rather than assuming a shared legal foundation.

Data governance in Africa, therefore, remains deeply fragmented. Thirty-seven AU member states have enacted personal data protection laws, yet definitions of personal data, cross-border transfer rules, and enforcement structures vary significantly.[84] Despite its adoption in 2014, the Malabo Convention has been ratified by only fifteen states, leaving its continental protections largely aspirational. Weak enforcement mechanisms further deepen legal fragmentation. Data Protection Authorities (DPAs), competition regulators, and IP offices often face chronic underfunding, limited digital forensics expertise, reliance on donor-funded technical support, challenges in supervising cross-border data flows, and insufficient capacity to engage global technology firms. These constraints create enforcement asymmetries that favour multinational platforms.

Even where strong statutes exist, enforcement gaps remain due to underfunded regulators, limited digital forensics expertise, lack of harmonised judicial interpretation, corruption and institutional capture, and gender-based exclusions and harm in digital participation. African women face distinct digital harms, including gender-based violence such as cyber harassment, image abuse and stalking.[85] They also experience surveillance of care work through household applications and discriminatory outcomes from biased algorithms in

83 IMF 'GDP, current prices', available at: https://www.imf.org/external/datamapper/NGDPD@WEO/ZAF/MAR/NGA/EGY/AFQ (viewed on 21 July 2025).

84 Data Policy Framework (n2).

85 N Nyabola *Digital Democracy, Analogue Politics* : *How the Internet Era is Transforming Politics in Kenya* (2018).

https://doi.org/10.47348/SAIPL/v13/i2a12

hiring, welfare, finance and policing.[86] Barriers such as limited digital literacy, high costs and restrictive cultural norms further exclude them from online platforms, while their invisibility in datasets produces inaccurate or harmful AI outputs. Digital systems often reproduce patriarchal structures and colonial hierarchies, while rights remain nominal without credible enforcement.

5.1 The AfCFTA as catalyst for legal harmonisation

The AfCFTA, the largest free trade agreement by membership since the establishment of the WTO, has completed Phase II negotiations, resulting in protocols on IP, investment, competition policy, and digital trade.[87] This marks the first continent-wide initiative to establish legally binding rules aimed at addressing the fragmented landscape of IP and data governance outlined in the previous section. The IP Protocol, adopted by the Council of Ministers in February 2023, is central to this effort. The Protocol sets minimum standards for copyrights, patents, trademarks, and geographical indications. It simultaneously integrates flexibilities that support development objectives. LDCs receive a three-year implementation grace period,[88] technology transfer aligns with TRIPS art 66.2,[89] and broader exceptions are allowed for education, research, and public health.[90] However, the IP Protocol is not yet in force, as it awaits member state ratifications and completion of technical annexes, leaving much of its content proposed rather than binding.

Additionally, the consolidated Digital Trade Protocol text from February 2024 includes provisions directly relevant to data governance. Article 20 requires state parties to facilitate data flows essential for digital trade, subject to a forthcoming annex that will outline permissible public policy exceptions.[91] This mechanism would replace 37 divergent national data transfer regimes with a unified continental authorisation framework. The Digital Trade Protocol also establishes baseline rules for cybersecurity[92] and consumer protection,[93] addressing regulatory gaps and reducing inconsistencies across sector-specific standards. However, the Trade Protocol is not yet in force, with ratification and annex development ongoing. Therefore, its provisions should be regarded as adopted text with future binding effect, not current enforceable obligations.

6. Data Ownership and Value Distribution on Digital Platforms

Africa's digital economy is marked by significant imbalances in value capture.[94] Despite contributing a growing share of global data flows, Africa retains under

86 Ibid.
87 Tralac 'AfCFTA negotiations timeline', available at: https://www.tralac.org/resources/afcfta-negotiations-timeline.html (accessed on 21 July 2025).
88 Article 35(2) of the IP Protocol (n74).
89 Ibid.
90 Ibid.
91 Article 20 of the AU Digital Trade Protocol (n47).
92 Ibid.
93 Ibid.
94 AU Digital Transformation Strategy (n29).

5% of the resulting economic value.[95] This disparity is most pronounced in the platform economy, where data from the United Nations Conference on Trade and Development (UNCTAD) show that 90% of the market capitalisation of the seventy largest digital platforms is concentrated in the United States and China.[96] This imbalance has fuelled critical debates on data colonialism, digital sovereignty, and equitable development in the global digital sphere. According to Couldry and Mejias, digital extractivism is the large-scale appropriation of behavioural and relational data, enabling global tech firms in Africa to extract economic value from local digital labour and data with little return to communities or domestic economies.[97] Examples include uncompensated scraping of African language corpora for AI training, extraction of geospatial and biometric data, value capture by platforms with minimal reinvestment, reliance on foreign cloud infrastructure, and concentration of digital advertising markets. Unlike oil or minerals, data does not physically leave the continent. Its extraction occurs through platform interfaces, metadata surveillance, algorithmic tracking, cloud offshoring, opaque contracts, and AI training pipelines. This creates an invisible data drain where African individuals, researchers, and creators supply the raw material for machine-learning models but gain little profit or control.

Africa's digital future must be understood within global political-economic structures shaped by colonial legacies, unequal knowledge flows, and technological power asymmetries. International IP law, rooted in European industrial interests and focused on individual authorship and market value, excluded African knowledge traditions that are communal, iterative, relational, and oral. African states have historically had limited influence over global digital-regulatory frameworks, resulting in poor understanding and underuse of the Agreement on TRIPS flexibilities, data-transfer rules that favour wealthier jurisdictions, and massive value extraction by global platform companies without reciprocal obligations.[98] Digital infrastructures such as cloud storage, undersea cables, algorithms, and platforms are concentrated in the Global North, creating a form of 'digital colonialism' where African data powers global AI systems while African countries struggle to achieve digital sovereignty, equitable value sharing, and fair access to machine-learning tools.

The AU's Data Policy Framework highlights three structural factors driving Africa's limited value capture in the digital economy. First, platform asymmetry allows dominant global firms to centralise high-margin data analytics and monetisation in offshore data centres.[99] Digital platforms such as e-commerce,

95 Ibid.

96 Digital Economy Report (n45).

97 N Couldry & UA Mejias *The Costs Of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism* (2019).

98 African states, as rule-takers in early global IP and digital-trade negotiations, inherited frameworks shaped by wealthier jurisdictions. This left governments with limited capacity to implement TRIPS flexibilities, little leverage to challenge restrictive data-transfer norms, and few tools to counter asymmetrical value extraction by dominant platforms.

99 Data Policy Framework (n2).

https://doi.org/10.47348/SAIPL/v13/i2a12

social media, ride-hailing, and online advertising rely on network effects and data accumulation. In Africa, they capture vast behavioural data, face little competition due to infrastructure and capital barriers, and return minimal value to local economies. This dynamic is reinforced by Africa's minimal share of global server capacity.[100] African firms often struggle to compete, not from lack of innovation but because platform dominance relies on data control rather than traditional IP. Second, tax misalignment allows profits to be allocated to the jurisdictions where digital platforms are domiciled, rather than to the markets generating the data. This results in a continued decline in domestic fiscal revenue. Third, fragmented governance is evident in divergent privacy laws and the limited ratification of the Malabo Convention. This fragmentation hinders the creation of a unified continental data market, raises compliance costs for local start-ups, and limits cross-border data analytics, reinforcing Africa's marginal role in the global digital value chain.

Africa's limited digital value capture carries significant developmental consequences. Due to ongoing legal uncertainties around data ownership and transferability, venture capitalists often apply a 20–30% discount to valuations of high-growth African technology firms.[101] This perceived risk limits investment and slows innovation. Moreover, the inability of local firms to aggregate data across jurisdictions hinders the development of regionally tailored AI models, deepening reliance on foreign technological infrastructure. Current policy responses in Africa's digital governance landscape can be categorised into three broad areas. The first involves data-sharing mandates, often referred to as 'secure API' or 'data access orders,' which would require dominant platforms to provide anonymised, standardised data interfaces to competitors and researchers. The second track focuses on fiscal realignment, with African countries engaging the OECD Pillar One framework to reallocate a portion of residual profits to the jurisdictions where data originates.[102] The third track focuses on regulatory harmonisation through the AfCFTA. Together, these measures aim to shift Africa's role from raw-data exporter to co-producer of data-driven value. However, their effectiveness will rely on timely ratification, strengthened technical capacity within enforcement agencies, and carefully crafted data-access mandates that safeguard legitimate trade-secret protections. The following sections therefore examine how a balanced legal framework can reconcile these competing imperatives in ways that are simultaneously protective and adaptive.

100 African Union (n59).

101 AVCA '2024 Venture capital reports in Africa', available at: https://www.avca.africa/media/pk1lhhzc/avca_2024_venture_capital_in_africa_report_rel-31-march.pdf (viewed on 22 July 2025).

102 OECD 'Multilateral convention to implement amount a of pillar one', available at: https://www.oecd.org/en/topics/sub-issues/reallocation-of-taxing-rights-to-market-jurisdictions/multilateral-convention-to-implement-amount-a-of-pillar-one.html (viewed on 22 July 2025).

7. Comparative Insights and Global Benchmarks

A comparative analysis highlights how various jurisdictions have attempted to balance proprietary incentives with the unrestricted flow of information. This effort can help shape Africa's reform trajectory, provided that legal transplants are carefully aligned with local institutional contexts. Adopting Global North IP frameworks without critical evaluation risks reinforcing colonial-era assumptions and neglecting Africa's communal creativity and informal innovation. Indigenous creative works such as stories, songs, and medicinal knowledge are shaped by communal participation and passed down through generations.[103] Western copyright law struggles to recognise such works because it demands a single identifiable creator, originality from individual skill, and fixation in material form. This results in under-protection of indigenous works and enables their over-appropriation by commercial actors. Africa must pursue knowledge sovereignty rather than mere protectionism, addressing the inadequacies of Western IP categories for African innovation, strengthening traditional knowledge governance, ensuring community-controlled data stewardship, and mitigating the risks of digital platforms appropriating indigenous data.

7.1 European Union (EU)

The EU's Digital Single Market strategy has established a comprehensive framework for platform and data governance through measures like the Digital Markets Act, which sets obligations for designated gatekeepers,[104] including interoperability,[105] API access,[106] data portability, [107]and bans on self-preferencing.[108] Two legislative instruments merit particular attention. Directive (EU) 2019/790 introduced mandatory rights for press publishers (art 15) and scientific research TDM (art 3), as well as an optional exception for lawful purposes (art 4).[109] Secondly, the EU Data Act grants users of connected devices a data portability right[110] and empowers national regulators to impose access obligations on gatekeeper platforms.[111] This approach embeds competition considerations within the broader framework of data governance.

103 Oguamanam (n79) 34.

104 Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act, 2022), arts 2–3, available at: https://eur-lex.europa.eu/eli/reg/2022/1925/oj/eng (viewed 21 November 2025).

105 Article 7 of Regulation (EU) 2022/1925 (n104).

106 Article 6(11) of Regulation (EU) 2022/1925 (n104)

107 Article 6(9) of Regulation (EU) 2022/1925 (n104).

108 Article 6(5) of Regulation (EU) 2022/1925 (n104).

109 Directive (EU) 2019/790 of the European Parliament and of the council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC.

110 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828, arts 4–5, available at: https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng (viewed 21 November 2025).

111 Articles 23–26 of Regulation (EU) 2023/2854 (n110).

https://doi.org/10.47348/SAIPL/v13/i2a12

Moreover, the Data Act sets the business-to-business (B2B)[112] and the business-to-government (B2G) data-sharing obligations, interoperability standards, and rules against unfair contract terms.[113] The EU experience demonstrates that African jurisdictions can effectively balance strong authorial rights with non-waivable research exceptions and prioritise data portability as a key component of consumer protection. These mechanisms could be modularly incorporated into AfCFTA annexes. This highlights Africa's need for TDM exceptions that remain technologically neutral, adaptable, and attentive to digital-development disparities.

7.2 The United States of America

In contrast, the United States adopts a more flexible approach through its broad and open-ended fair use doctrine codified in 17 USC § 107.[114] This doctrine permits transformative uses of copyrighted material, provided that the purpose, amount used, and market impact favour legitimacy. Landmark cases such as *Authors Guild v Google*[115] and *Kelly v Arriba Soft*[116] have interpreted fair use expansively, protecting large-scale digitisation and the use of image thumbnails in search engines. More recently, US courts have extended the doctrine to cover machine learning training sets, finding ingestion of copyrighted text transformative when outputs do not substitute the originals, as in *Andersen v. Stability AI*.[117] For African lawmakers, the US model demonstrates how open-textured doctrines can complement fixed statutory exceptions in common-law systems. This approach may help copyright frameworks adapt to emerging technologies. However, successful legal transplants require judicial capacity-building, as applying open-ended standards effectively depends on a skilled and consistent judiciary.

7.3 Brazil

The Brazilian Lei Geral de Proteção de Dados Pessoais (LGPD) offers a balanced approach between data localisation and the free flow of information. The LGPD allows cross-border data transfers to jurisdictions that ensure adequate data protection.[118] It also recognises standard contractual clauses and binding corporate rules as viable alternatives, helping avoid rigid localisation while preserving national control over data governance.[119] A key feature of the LGPD is the creation of the independent National Data Protection Authority (ANPD), empowered to enforce compliance and guide data governance through regulation and oversight.[120] The law further introduces graduated,

112 Article 22 of Regulation (EU) 2023/2854 (n110).
113 Article 15 of Regulation (EU) 2023/2854 (n110).
114 7 USC § 107 (2018).
115 *Authors Guild v. Google, Inc* No. 13-4829 (2d Cir. 2015).
116 *Kelly v. Arriba Soft Corp* 336 F.3d 811 (9th Cir. 2003).
117 *Andersen v Stability AI Ltd* (ND Cal, 2024).
118 Articles 33–36 of the General Personal Data Protection Act.
119 Ibid.
120 Ibid.

risk-based sanctions ranging from warnings to fines of up to 2% of a company's turnover.[121] These institutional and enforcement tools are especially relevant for African regulators operating under resource constraints. A single, specialised authority with proportionate penalties can boost regulatory effectiveness by enhancing deterrence and reducing administrative burden. Additionally, Brazil offers a Global South model of data protection that balances user rights with economic needs. Unlike the EU's adequacy mechanism, Brazil uses a flexible mix of contractual safeguards and institutional oversight, making it better suited to Africa's infrastructural constraints.

8. Translating Global Experience into an Afro-Centric Regulatory Blueprint

The appeal of adopting comprehensive Northern legal frameworks to unify Africa's fragmented digital regulations is understandable. However, historical experience counsels caution. Legal transplants adopted wholesale often prove ineffective when confronted with local political dynamics, constrained resources, and distinctive knowledge systems. A more pragmatic approach involves identifying core design principles from effective foreign models and tailoring them to Africa's institutional context. These principles function as essential components of a system, rather than representing its entirety. African digital economies are shaped by informal markets, limited IP enforcement, linguistic and cultural diversity, varied knowledge systems, and uneven digital infrastructure. These realities require flexible regulation rather than rigid harmonisation.

Uncritical adoption of global frameworks risks entrenching platform monopolies, limiting African AI innovation, excluding local creators from digital markets, and outsourcing regulatory interpretation to foreign courts. Global North frameworks assume individual authorship, exclusive ownership, market-based incentives, and formal registration systems, which do not align with African epistemologies. Many African IP statutes are colonial inheritances, and without decolonial reform, digital regulation risks reproducing extractive relationships through data mining without benefit-sharing, appropriation of traditional knowledge for AI training, concentration of African digital markets in multinational platforms, and the absence of Indigenous governance mechanisms.

The EU's DSM agenda shows how sector-specific issues can be addressed through targeted legal tools without disrupting the broader legal framework. Directive 2019/790 introduced two key measures: a mandatory neighbouring right for press publishers (art 15), requiring licensing talks with platforms, and a compulsory TDM exception for scientific research (art 3), extended by an optional exception for any lawful use (art 4). For Africa, the most relevant feature is the non-waivable TDM exception. Kenya's Copyright Act 2001 (amended in 2022) shows local feasibility, while pilot programmes in South

121 Ibid.

https://doi.org/10.47348/SAIPL/v13/i2a12

Africa and Nigeria can help refine scope and compensation before wider adoption under the AfCFTA.

By contrast, US fair use law under 17 USC § 107 permits transformative uses, including large-scale digitisation and image-search thumbnails, as upheld in *Authors Guild v. Google* and *Kelly v. Arriba Soft*. A recent case, *Andersen v. Stability AI*, suggests fair use may extend to machine-learning ingestion when outputs do not reproduce original content, though courts are still evaluating the boundaries of such use. African common-law jurisdictions could draw on this adaptable approach to modernise their statutes, particularly in contexts where legislative agility is limited. However, its success relies on well-resourced specialist IP courts to maintain coherent jurisprudence. Courts in many African jurisdictions struggle with insufficient training in handling digital evidence, significant backlogs caused by limited judicial resources, challenges in assessing algorithmic systems and complex economic evidence, and the absence of specialised courts or benches for IP and digital matters.

Brazil's LGPD adopts a balanced approach to data localisation, combining national data sovereignty with flexible cross-border transfer mechanisms inspired by the EU's General Data Protection Regulation. It permits cross-border data transfers via adequacy decisions, standard contractual clauses, or binding corporate rules. This framework safeguards national sovereignty while reducing barriers to digital trade. The law establishes an independent data protection authority known as the ANPD, which is funded through earmarked levies and has the power to impose graduated sanctions, including fines of up to two per cent of a company's turnover. For African regulators facing resource constraints, Brazil's model demonstrates how institutional independence and proportionate penalties can be aligned with flexible data transfer rules. Under art 20 of the AfCFTA Digital Trade Protocol, an African Passport could implement a multi-layered data transfer mechanism, supported by an independent authority modelled on Brazil's ANPD to ensure credibility and effective enforcement.

9. Policy and Legislative Roadmap Aligned with Sustainable Development Goal 9

The reform path proposed in this article rests on the principle that legal change should be evidence-based, context-sensitive, and institutionally grounded. SDG 9, which promotes resilient infrastructure, inclusive industrialisation, and innovation, serves as the primary benchmark for evaluation.[122] Instead of adopting comprehensive legal codes from the Global North, the proposed roadmap prioritises regulatory sandboxes, modular reforms, and independent oversight institutions. This approach addresses postcolonial critiques of legal imperialism while meeting the AfCFTA's demand for evidence-based regulation. Under art 23(a) of the Digital Trade Protocol, member states may

122 United Nations 'The 17 Sustainable Development Goals (United Nations Sustainable Development', available at: https://sdgs.un.org/goals (viewed 21 November 2025).

create pilot frameworks such as sandboxes to foster innovation, competition, and cross-border digital trade.[123] In Africa, these sandboxes act as transitional mechanisms that bridge fragmented national laws and pave the way for future continental harmonisation.

The AfCFTA Digital Trade Protocol promotes innovation-friendly regulation, and regulatory sandboxes in South Africa, Kenya, and Nigeria operationalise this by enabling innovators to test products under proportionate oversight. Participation in these sandboxes requires two core commitments. First, participants must publish anonymised APIs that are fairly, reasonably, and non-discriminatorily priced. Second, they must submit algorithmic impact assessments for review by joint ARIPO–OAPI panels. These conditions ensure that experimental activities generate detailed data on costs, bias, and interoperability challenges. The resulting evidence directly supports SDG 9. It also contributes to Indicator 9.5.1, which tracks research and development expenditure as a share of GDP, by reducing prototyping costs. It also supports Indicator 9.c.1, which tracks mobile network coverage, by promoting open interfaces that broaden access for SMEs. However, sandboxes can enable regulatory capture by multinationals, exclude local innovators, weaken personal data safeguards, and inadvertently legitimise exploitative digital practices.

Sandbox findings inform targeted statutory reforms, avoiding wholesale adoption of foreign legal frameworks. Sandboxes address institutional scarcity by allowing regulators to test complex digital issues such as TDM, AI training, and cross-border data flows without fully developed statutory frameworks or extensive capacity. They mitigate risks from rapid technological change by providing a controlled space to gather evidence before enacting binding rules. Sandboxes also support harmonised standards by enabling states to experiment with similar regulations and report to the AfCFTA Secretariat under art 50 peer review, fostering convergence in digital governance. Additionally, they can incorporate African epistemologies and community values by integrating traditional knowledge, Indigenous governance, gender checks, and benefit-sharing frameworks.

Triggers for compulsory licensing in AI are calibrated using cost data from sandbox testing. Guided by the COMESA Draft Digital Markets Guidelines, competition authorities in all three countries regard unjustified refusals to provide fair, reasonable, and non-discriminatory APIs as abuses of market dominance. This approach integrates competition principles with existing trade secret protections. Simultaneously, DPAs are transforming into independent agencies with dedicated funding and board-level governance, inspired by the model of Brazil's National Data Protection Authority. These reforms enhance enforcement capabilities and promote the application of proportionate penalties. Collectively, these initiatives support SDG 9, specifically targets 9.1

123 Article 23(a) of the AU Digital Trade Protocol (n47).

https://doi.org/10.47348/SAIPL/v13/i2a12

and 9.b, by strengthening trusted digital infrastructure and fostering robust domestic research ecosystems.

A data tax framework modelled on the OECD Pillar One approach reallocates the residual profits of digital multinationals to the jurisdictions where their users are located. This approach broadens fiscal capacity for investments in broadband infrastructure and digital skills development, both of which are vital to building resilient infrastructure. At the same time, constitutional or legislative amendments are being introduced to enshrine the rights to privacy, data portability, and algorithmic fairness. These changes elevate digital rights from policy goals to enforceable legal claims. Together, these reforms promote inclusivity and sustainability, reinforcing the role of IP and data governance in advancing inclusive industrialisation under SDG 9.

According to art 50 of the Digital Trade Protocol, best-practice provisions validated in South Africa, Kenya, and Nigeria must be submitted for review at the continental level. This built-in mechanism for diffusion allows AU Member States to adopt modular reforms such as TDM exceptions, fair and reasonable access to APIs, and data portability rights, without imposing a uniform legal framework. This roadmap links local experimentation with AfCFTA harmonisation, enabling Africa to advance SDG 9 through evidence-based, context-sensitive regulation rather than replicating foreign legal systems.

9.1 Criteria and safeguards for the four regulatory dials

This paper aims to translate the protective–adaptive blueprint into a practical legal and regulatory framework to guide decision-making across diverse African jurisdictions. The aim is to operationalise the blueprint so regulators, courts, policymakers, and AfCFTA bodies can apply it with clarity and precision. Each dial is governed by five elements. Activation thresholds define the conditions that trigger intervention, such as dominance, essentiality, irreproducibility, lawful access, or public-interest necessity. Legal tools specify the statutory or regulatory mechanism for implementation. Oversight and appeals identify the competent authority and its appeal route. Safeguards include protections for trade secrets, privacy, traditional knowledge, due process, cybersecurity, FRAND pricing, and proportionality. Success metrics provide measurable indicators such as SME onboarding time, data-access costs, interoperability, research outputs, and bias reduction. This structure ensures consistency across all four dials.

9.2 Patents and compulsory licensing

This dial applies when a patent covers technology essential for digital market participation, such as encryption protocols, AI inventions, or telecom standards, and the holder is dominant, replication is infeasible, and refusal to license harms innovation, competition, or public welfare. The legal tool is a compulsory licence or government-use order under national law, supported by TRIPS flexibilities and AfCFTA IP principles. Oversight begins with the national IP office, with appeals to the High Court and then the Supreme Court

of Appeal or Constitutional Court. Safeguards include trade-secret protection, FRAND-based remuneration, purpose limitation, audit rights, and time-bound access. Success is measured by lower technology costs, greater SME participation, and accelerated digital innovation.

9.3 Copyright and text and data mining (TDM)

The activation threshold applies when the use serves research, teaching, innovation, or preservation of African languages and cultural heritage, provided the works are lawfully accessed and copying is non-expressive without substituting market demand. This ensures contextual fit rather than over-generalising. The legal tool may be a statutory TDM exception or a regulated research licence, overseen by a national copyright authority or Tribunal with appeals to the High Court. Safeguards include de-identification audits, secure research environments, exclusion of traditional knowledge or sacred materials, privacy-by-design, and remuneration for commercial use. Success is measured by research outputs, growth of African-language datasets, legal certainty for AI developers, and improved academic accessibility.

9.4 Trade secrets and secure, interoperable API access

The activation threshold applies when a platform is dominant under competition-law benchmarks, controls a non-replicable API or digital interface, and refusal to supply forecloses competitors or undermines public interest — examples include messaging APIs, mobile-money APIs, or social-media authentication systems as digital essential facilities. The legal tool is a competition-law access order with FRAND-based or non-discriminatory terms under s 8 of the Competition Act, overseen by the Competition Commission, adjudicated by the Competition Tribunal, and appealable to the Competition Appeal Court. Safeguards include encryption standards, trade-secret protection, audit logs, cybersecurity measures, rate limiting, multilayered authentication, and strict purpose limitation. Success metrics focus on improved interoperability, reduced SME onboarding times, increased competition, and fewer exclusionary outcomes, especially in fintech, mobility, and communications markets.

9.5 Database rights and open licences

The activation threshold applies when datasets involve publicly funded research, linguistic resources, or essential digital inputs such as agricultural or geospatial data, provided privacy risks are mitigated, and Indigenous communities grant free, prior, informed, and ongoing consent where relevant. The legal tool consists of open-data licences, including Traditional Knowledge-sensitive licences with cultural integrity and benefit-sharing conditions. Oversight is provided by the Information Regulator, National Archives, and Traditional Knowledge Councils, with judicial review for contested decisions. Safeguards include Free Prior Informed Consent processes, privacy-by-design, differential privacy, benefit-sharing arrangements, protection for sacred or culturally sensitive materials, and limits on commercial reuse. Success metrics include

https://doi.org/10.47348/SAIPL/v13/i2a12

greater dataset diversity, increased availability of African-language and African-context data for AI, enhanced ethical AI development, and measurable community benefits.

10. Conclusion

Africa's digital economy is reaching a defining point in its development. Africa can either continue exporting raw data and talent or evolve into a producer of high-value knowledge goods. This paper argues that the determining factor is not technological capability alone, but rather the quality of the legal and institutional frameworks that shape incentives and access. As Africa integrates into global data flows and AI-driven innovation, it must address structural inequalities rooted in colonial IP regimes, weak regulation, and power imbalances with multinational tech firms. The paper argues that Africa needs an adaptive, context-driven regulatory framework to achieve digital sovereignty, protecting creators, communities, and consumers while fostering innovation, research, and cross-border digital trade. The paper proposes a model that balances protection and adaptability, structured around four regulatory pairs. These pairs include patents and compulsory licences, copyright and TDM, trade secrets and secure API access, and database rights and open licences. Rather than enforcing exclusivity or treating data as a global commons, this model reflects African realities such as communal authorship, informal innovation markets and urgent development needs.

Regulatory sandboxes under AfCFTA Digital Trade Protocol art 23(a) act as a bridge between national experimentation and continental harmonisation. Together with arts 20 and 50, sandboxes provide African jurisdictions a mechanism to coordinate regulatory learning, prevent premature harmonisation, and reduce multinational capture through transparency, multi-stakeholder oversight, and context-sensitive evaluation. They produce empirical metrics, including cost curves, bias audits and FRAND benchmarks, which are necessary to adjust each regulatory pair with accuracy. These results inform flexible statutory reforms and competition-sensitive regulation, avoiding the rigid legal structures often criticised by postmodern and decolonial IP scholars. This approach respects both financial limitations and the decolonial emphasis on gradual and locally grounded reform. Fiscal coordination through a data tax framework similar to the OECD model, along with constitutional or legislative protections for privacy, data portability and algorithmic fairness, helps safeguard these reforms from future policy reversals. Additionally, by linking each stage of the roadmap to SDG 9, which focuses on resilient infrastructure, inclusive industrialisation and innovation, the paper places legal reform within a measurable development framework. Reductions in patent filing costs, expansion of open APIs and new revenue streams from digital taxation provide clear indicators for assessing progress. If implemented, the roadmap could transform the projected $1.5 trillion digital dividend into widespread social and economic benefits, helping to close the continent's data value gap while preserving its rich knowledge commons. Africa cannot afford

to replicate Northern legal systems without adaptation, and it equally cannot afford to remain inactive. The protective and adaptive model offers a balanced approach that is grounded in evidence, responsive to context and aimed at inclusive growth driven by innovation.

https://doi.org/10.47348/SAIPL/v13/i2a12