MZALENDO

BUILDING A RESILIENT KENYA

THE MALABO CONVENTION AS A FRAMEWORK FOR CYBERSECURITY, DATA PROTECTION, AND CONTINENTAL TRADE

RECIPE
Recentering The Civic Internet Through Partner Engagement

Co-funded by the European Union

OXFAM

BUILDING A RESILIENT KENYA

THE MALABO CONVENTION AS A FRAMEWORK FOR CYBERSECURITY, DATA PROTECTION, AND CONTINENTAL TRADE

MZALENDO TRUST
P. O. BOX 21765
Nairobi, Kenya

Disclaimer
This publication was co-funded by the European Union. Its contents are the sole responsibility of Mzalendo Trust and do not necessarily reflect the views of the European Union.

RECIPE Recentering The Civic Internet Through Partner Engagement
Co-funded by the European Union
OXFAM
MZALENDO

Acknowledgements

This Policy Brief was commissioned by Mzalendo Trust and Oxfam Kenya as part of the Recentering the Civic Internet through Partner Engagement (ReCIPE) project, co-funded by the European Union. The ReCIPE project seeks to strengthen rights-respecting digital ecosystems by supporting civil society engagement in digital governance and digital rights processes across multiple regions. We also acknowledge the partnership and technical support of colleagues from Oxfam, including Jane Muhia, Susana Castano, Mia Marzotto, Bill Marwa, Hood Lubowa, Nogaye Ndoye, and Khady Seck Diop, whose contributions helped strengthen the analytical clarity and policy relevance of this publication.

We acknowledge the leadership of Ms. Caroline Gaita, Executive Director of Mzalendo Trust, and the broader Mzalendo team for their institutional guidance, technical review, and continued commitment to advancing open, inclusive, and accountable governance in Kenya.

This Policy Brief was researched and written by Ephraim Percy Kenyanito, with research assistance from Demas Kiprono, and coordination and editorial support from Gitungo Wamere, Grace Naiserian, and Vallary Acholla of Mzalendo Trust. The analysis draws on desk research and Key Informant Interviews conducted in August 2025 with stakeholders from the Office of the Data Protection Commissioner, the Media Council of Kenya, the Communications Authority of Kenya, the Bloggers Association of Kenya, the Data Protection Governance Society of Kenya, Amnesty International Kenya, as well as independent experts in law, technology, legal informatics, and digital rights in East Africa. We are grateful to all interview participants who generously shared their time, expertise, and perspectives, which greatly informed the analysis presented in this publication.

Note on the Cabinet Decision

Following the preparation of the research for this Brief, the Cabinet of Kenya approved a process step towards accession to the Malabo Convention in September 2025. The Office of the Data Protection Commissioner (ODPC) subsequently led broad national stakeholder consultations (deadline: 6 October 2025). This is a significant and welcome development. This Brief was originally commissioned in anticipation of and in support of this process. Its recommendations regarding legislative alignment, implementation resourcing, civil society engagement, and the 'Malabo Plus' approach now serve as inputs to the implementation of the process step towards accession rather than to the ratification debate.

List of Abbreviations

AfCFTA: African Continental Free Trade Area
AI: Artificial Intelligence
ANCS: Agence Nationale de la Cybersécurité (National Cybersecurity Agency, Tunisia)
ARTP: Autorité de Régulation des Télécommunications et des Postes (Regulatory Authority for Telecommunications and Posts, Senegal)
AU: African Union
CA: Communications Authority of Kenya
CDP: Commission de Protection des Données Personnelles (Commission for Personal Data Protection, Senegal)
CERT: Computer Emergency Response Team
CIRT: Computer Incident Response Team
CMCA: Computer Misuse and Cybercrimes Act (Kenya)
CSA: Cyber Security Authority (Ghana)
CSO: Civil Society Organisation
DCSSI: Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information (Directorate General for Cryptography and Information Systems Security, Senegal)
DPA: Data Protection Act (Kenya)
DPC: Data Protection Commission (Ghana)
DPO: Data Protection Office (Rwanda)
EAC: East African Community
ECOWAS: Economic Community of West African States
EU: European Union
GDPR: General Data Protection Regulation (European Union)
HRD: Human Rights Defender
ICCPR: International Covenant on Civil and Political Rights
ICT: Information and Communication Technology
INPDP: Instance Nationale de Protection des Données Personnelles (National Authority for the Protection of Personal Data, Tunisia)
KE-CIRT/CC: Kenya Computer Incident Response Team Coordination Centre
KICA: Kenya Information and Communications Act
KII: Key Informant Interview
MLAT: Mutual Legal Assistance Treaty
NC4: National Computer and Cybercrimes Co-ordination Committee (Kenya) (statutory name under CMCA section 4)
NCSA: National Cyber Security Authority (Rwanda)
NDT: New Deal Technologique (Senegal)
NITA-U: National Information Technology Authority — Uganda
ODPC: Office of the Data Protection Commissioner (Kenya)
OGP: Open Government Partnership
OGBV: Online Gender-Based Violence
PDPO: Personal Data Protection Office (Uganda)
ReCIPE: Recentering the Civic Internet through Partner Engagement
SME: Small and Medium-Sized Enterprise
VASP: Virtual Asset Service Provider
WTO: World Trade Organization

Table of **Contents**

Table of Contents

Executive Summary

Kenya stands at a definitive digital crossroads. Often lauded as the 'Silicon Savannah', the country has successfully built the hard infrastructure of a thriving digital economy, a trajectory shaped by a unique brand of 'political entrepreneurialism' that catalysed innovation in the early 2000s.[1] This ecosystem is exemplified by the ubiquity of M-Pesa and a rapidly expanding Information and Communication Technology (ICT) sector, which has fundamentally shifted paradigms in creativity and technology diffusion.[2] As the European Union (EU) and other global powers seek digital partnerships with Africa, Kenya has positioned itself as a primary node in this emerging network, navigating a complex web of global rivalries.[3]

This digital transformation has revolutionised financial inclusion and service delivery, creating 'industries without smokestacks' that offer a new developmental model for the continent.[4] However, rapid growth has outpaced the development of a unified, rights-respecting safety framework, leaving the ecosystem vulnerable to escalating cyber threats and legislative fragmentation.

Furthermore, an important governance challenge remains: ensuring that legitimate digital security interests and the protection of constitutional rights advance together. Kenya's technical community, legal practitioners, and civil society have consistently highlighted that a continental rights-based framework would complement existing domestic legislation and help maintain the broad public trust that sustains Kenya's digital economy. [9,10]

The Malabo Convention, the African Union (AU) Convention on Cyber Security and Personal Data Protection, offers a ready-made blueprint to bridge these gaps.[11] As a comprehensive continental framework, it harmonises three critical pillars: cybersecurity, personal data protection, and electronic transactions.[12] Ratification is not merely a diplomatic formality; it is a strategic economic imperative. As a senior ODPC official noted in consultations for this brief: 'Ratifying will send a strong signal that Kenya is a destination to invest in technologically ... and is a destination where it is easy to do business.'[8]

With the operationalisation of the African Continental Free Trade Area (AfCFTA) Protocol on Digital Trade, regulatory convergence is essential.[15] Kenya risks finding its data regime classified as 'inadequate' for these regional flows, effectively compromising its economic sovereignty and competitive edge, if it cannot align with continental standards.[16] As a senior official of the Communications Authority of Kenya (CA) observed, Malabo provides the 'international bridge' that Kenya's national laws need to be effective against global threats.[120]

Comparative analysis of five African peers reveals divergent paths that offer critical lessons. Senegal and Ghana, early ratifiers, demonstrate that harmonised frameworks attract investment and streamline incident response through robust institutions such as Ghana's Cyber Security Authority (CSA). Rwanda exemplifies the economic potential of integration, successfully linking its digital governance strategy directly to trade facilitation and digital exports. Conversely, Uganda and Tunisia — non-ratifiers — illustrate how, in the absence of binding supranational commitments, cybercrime laws may, absent regional safeguards, be applied in ways that constrain civic space and limit freedom of expression.

Despite the clear benefits demonstrated by its peers, Kenya remains among the non-ratifiers. The Attorney General (AG) has formally cleared the Convention for ratification, but the process has stalled twice due to successive cabinet reshuffles, a bureaucratic, not principled, obstacle.[8] This Policy Brief argues that domestic frameworks alone cannot fully address the challenges of cross-border digital governance and recommends a 'Malabo Plus' approach: ratifying the Convention while enacting targeted domestic reforms to safeguard human rights and streamline enforcement.

Key Recommendations

Government:

Conduct a formal 'Legislative Gap Analysis' to align the Data Protection Act (DPA) and Computer Misuse and Cybercrimes Act (CMCA) with Malabo; expedite ratification with interpretative declarations to protect national interests; and enact a 'Malabo Implementation Act' incorporating Article 25(3) human-rights safeguards into the Computer Misuse and Cybercrimes Act (CMCA).

Civil Society:

Shift from general opposition to constructive advocacy, proposing specific legal safeguards for marginalised groups — including women, youth, and persons with disabilities — to be attached to the ratification instrument.

Private Sector:

Frame ratification as a compliance cost-reduction mechanism that harmonises obligations across the continent, unlocking the full potential of the African Continental Free Trade Area (AfCFTA) Digital Single Market.

African Union (AU):

Urgently institutionalise the Article 32 implementation follow-up mechanism by establishing a permanent Convention Secretariat within the AU Commission with human-rights, AI, and biometrics expertise; produce regular public implementation reports; and host regional best-practice forums.

Introduction

A. Methodology, Purpose and Objectives

This Policy Brief serves as an advocacy tool under the Recentering the Civic Internet through Partner Engagement (ReCIPE) project — co-funded by the European Union (EU) and launched in mid-2024 by Oxfam and civil society partners to cultivate rights-respecting digital ecosystems across ten countries, including Kenya.[17] It draws on desk research and Key Informant Interviews (KIIs) conducted in August 2025 with senior stakeholders across government, civil society, the media, and independent legal practice in Kenya. Participants provided informed consent.

The Brief's objectives are: (i) to raise awareness of the Convention's principles, provisions, and continental importance; (ii) to highlight ratification and implementation status in Kenya and comparator states; (iii) to identify challenges, barriers, and opportunities using Kenya as a case study; (iv) to conduct comparative assessments against Kenyan laws to identify gaps and complementarities; (v) to offer tailored recommendations for government, civil society, academia, the private sector, and the African Union (AU); and (vi) to explore implications of regional frameworks including the AfCFTA Digital Trade Protocol, the Economic Community of West African States (ECOWAS) Supplementary Act, and the East African Community (EAC) Data Protection Bill.

B. Introduction to the Malabo Convention: Aims and Concerns

The Malabo Convention, officially known as the African Union Convention on Cyber Security and Personal Data Protection, was adopted on 27 June 2014 during the 23rd Ordinary Session of the African Union (AU) Assembly in Malabo, Equatorial Guinea.[19] Its stated purpose is to create a unified legal framework for cybersecurity, personal data protection, and electronic transactions, addressing the continent's fragmented regulatory environment. The Convention entered into force on 8 June 2023 after Mauritania's ratification as the 15th state. As at March 2026, 20 African Union (AU) member states have ratified it — while key players such as Kenya have neither signed nor ratified, contributing to ongoing regulatory disparities.[20] Civil society engagement with the Convention began immediately upon its adoption. Access Now's Sub-Saharan Africa team tracked the Convention's development from the pre-adoption drafting stage, publishing early analyses of both the regional momentum it represented[171,172] and the rights risks embedded in emerging implementing legislation.[173] This civil society record of monitoring the Convention from its inception provides the evidentiary foundation for the implementation concerns set out in this Brief.

The Convention's three pillars are: (i) Personal Data Protection (Articles 9–23), mandating independent national authorities, principles of consent and data minimisation, and transborder-flow regulations; (ii) Cybersecurity and Cybercrime (Articles 24–31), requiring national cybersecurity strategies and criminalisation of offences such as hacking, fraudulent access, child pornography, and hate speech, with safeguards under Article 25(3) to protect fundamental rights including freedom of expression, privacy, and the right to a fair hearing; and (iii) Electronic Transactions (Articles 2–7), governing the scope of electronic commerce, advertising, contractual obligations, and the functional equivalence of electronic and paper-based instruments.

Proponents argue the Convention fosters African ownership in digital spaces, reducing reliance on external norms such as the Budapest Convention, and supports economic integration via the African Continental Free Trade Area (AfCFTA).[21] However, significant criticisms persist: vague cybercrime definitions (e.g., 'cyber-terrorism' and 'cyber-harassment') risk over-criminalisation and unintended restriction of lawful expression; the Convention lacks mandatory data breach notification requirements; Article 11 criteria for authority independence are insufficiently detailed; and there is limited attention to emerging technologies such as Artificial Intelligence (AI).[16] Civil society reports also identify concerns over potential surveillance in international cooperation without adequate due-process safeguards.[17]

The State of
Digital Governance in Kenya

Kenya occupies a prominent position in Africa's digital landscape, frequently referred to as the 'Silicon Savannah'.[24] The National Digital Master Plan 2022–2032 targets the digitalisation of 80% of government services and deployment of 100,000 km of fibre optic infrastructure.[25] M-Pesa, launched in 2007, has enabled over 89% of the adult population to engage in digital payments, remittances, and micro-lending.[29] The Information and Communication Technology (ICT) sector has grown at an average annual rate of 10.8%, with the digital economy projected to contribute approximately 9.24% to Gross Domestic Product (GDP) by end 2025.[27]

These advancements have amplified vulnerabilities. Kenya recorded 2.54 billion cyber threat events in Q1 2025–2026, with estimated losses of KSh 29.9 billion from ransomware, phishing, and malware — a 20% year-on-year increase in cyberattacks.[32,33] This underscores the imperative for harmonised regulatory measures.

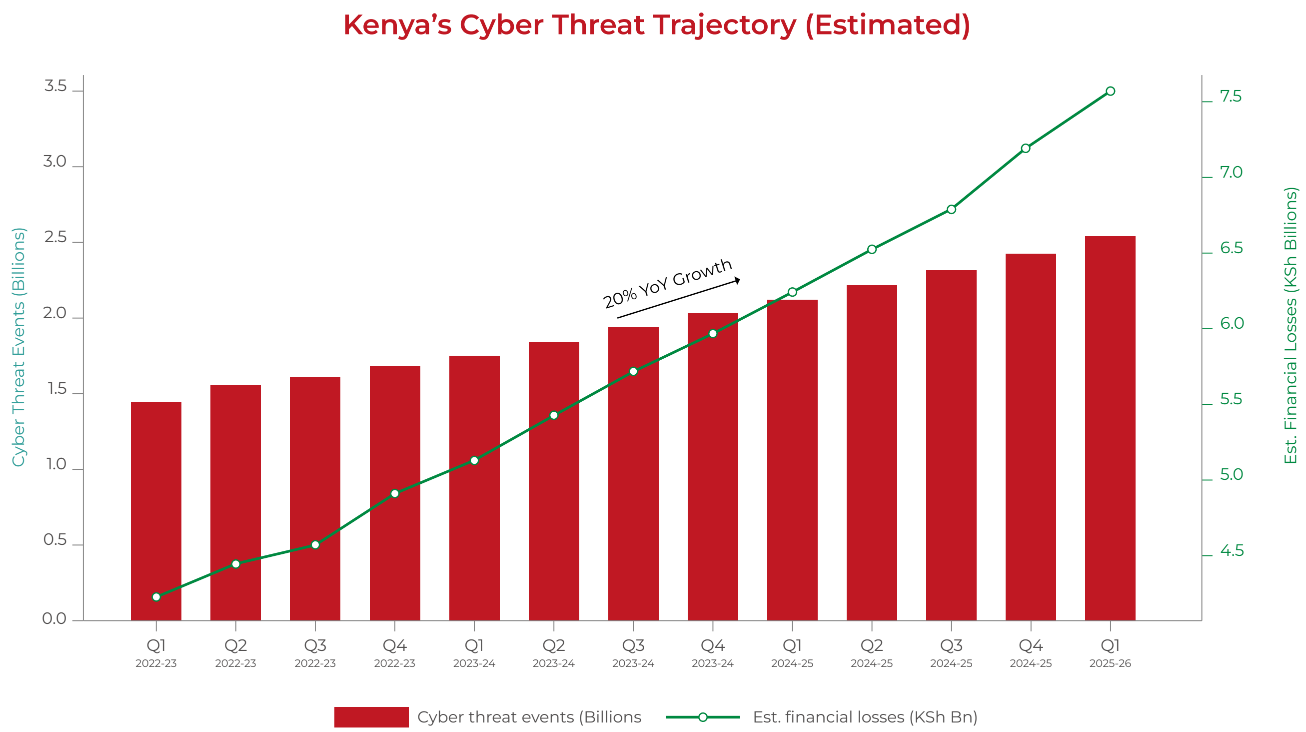


Figure 1: Kenya's Cyber Threat Trajectory (Estimated), Q1 2022–2023 to Q1 2025–2026.
Source: Communications Authority of Kenya, Sector Statistics Reports 2020–2025;
CA Kenya Cyber Threat Report Q1 2025/2026 (endnotes 32, 33)

Figures 1.1 and 1.2 contextualise these developments: the rapid growth of Kenya's digital economy over the past decade has been matched by an escalating cybercrime cost — underscoring why the cooperation architecture that Malabo provides has become urgent.

Kenya: Digital Economy Growth vs. Cybercrime Cost 2013-2025
ICT sector contribution to GDP (%) and estimated cybercrime losses (KSh Billions)

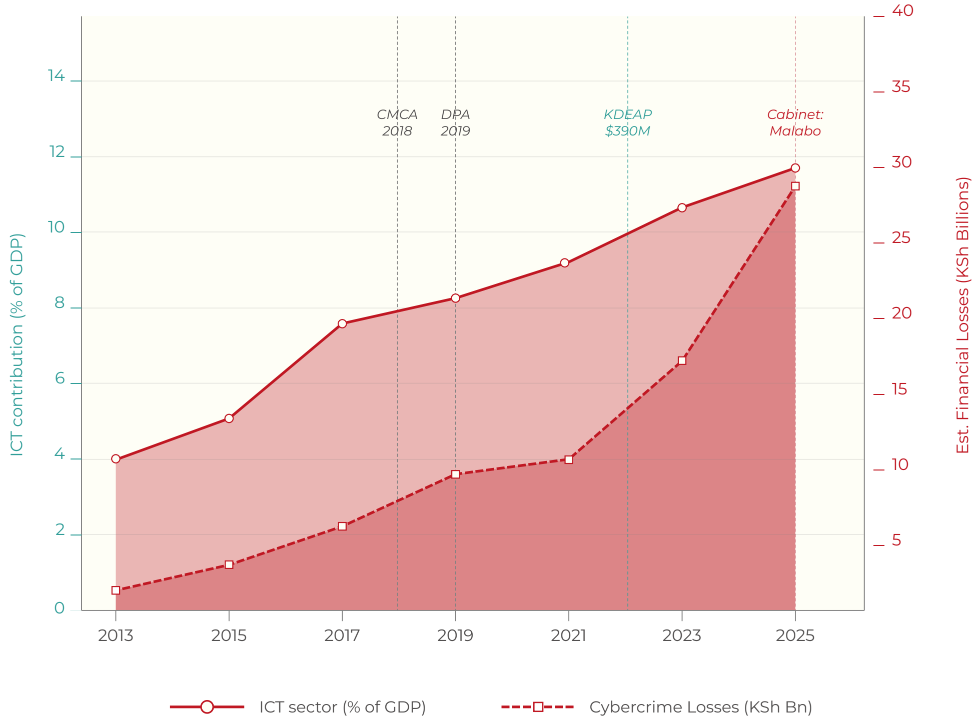


Figure 1.1: Kenya Digital Economy Growth vs. Cybercrime Cost 2013–2025. ICT sector contribution to GDP (%, left axis) vs estimated cybercrime losses (KSh billions, right axis). Sources: ICT/GDP: KNBS; World Bank KDEAP documentation (9.24%, 2022, EN 179). Cybercrime losses: Serianu Africa Cybersecurity Reports 2019–2024; CA Kenya Cybersecurity Report Q1 2025/26 (KSh 29.9bn, EN 183).

Kenya Mobile Economy Expansion 2013–2025.
Mobile money transaction value (KSh trillions per year) and mobile internet users (millions).

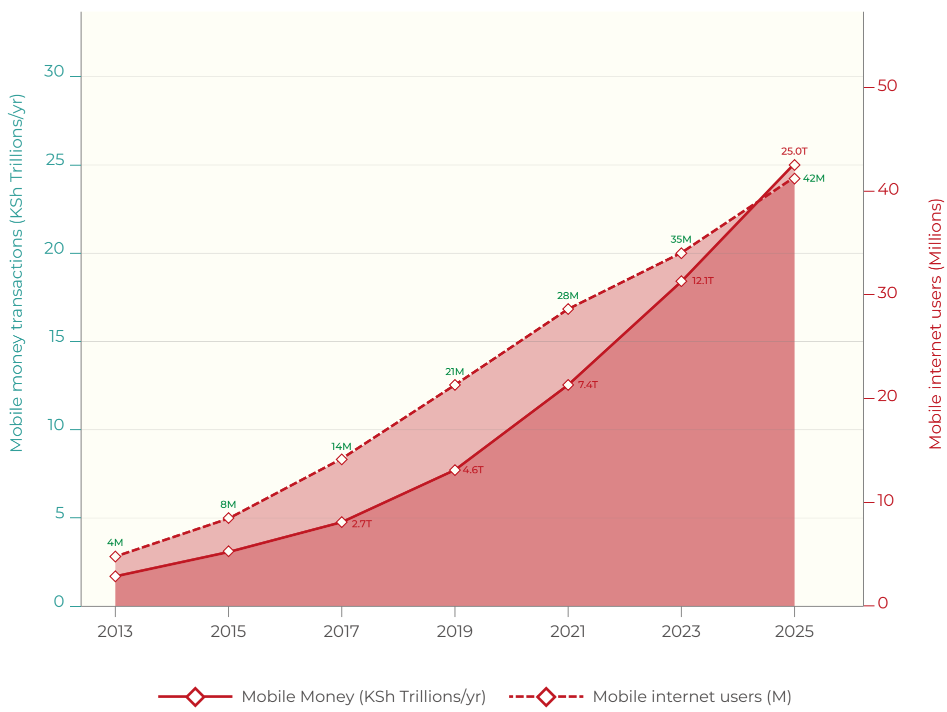


Figure 1.2: Kenya Mobile Economy Expansion 2013–2025. Mobile money transaction value (KSh trillions per year) and mobile internet users (millions). AfCFTA digital market projected at $712 billion by 2050. Sources: CBK Annual Reports (2013–2025, EN 27); GSMA Kenya Digital Economy Report Oct 2024 (EN 181); CA Kenya sector statistics; Serianu/PwC cited in Ecofin Agency (EN 183).

Kenya's framework rests on three pillars: data protection (Data Protection Act (DPA) 2019), cybersecurity (Computer Misuse and Cybercrimes Act (CMCA) 2018, amended 2025), and electronic transactions (Kenya Information and Communications Act (KICA) 1998). Following Cabinet approval of a process step towards accession to the Malabo Convention in September 2025, the Office of the Data Protection Commissioner (ODPC) has led broad national stakeholder consultations. As at the date of this Brief, the formal accession process is ongoing. Alignment is partial, with significant gaps in rights safeguards and harmonisation, as Table 1 summarises.

MALABO PILLAR	KENYAN ALIGNMENT	KEY GAPS
Personal Data Protection (Arts 9–23)	Strong: Data Protection Act (DPA) 2019 enshrines consent, purpose limitation, data subject rights, and independent Office of the Data Protection Commissioner (ODPC).	Data Protection Act (DPA) fines (max KSh 5 million / 1% turnover) insufficiently deterrent for large data controllers. No mandatory breach-notification timelines. No Artificial Intelligence (AI)-specific rules. 90-day investigation limit hampers complex cases. DPA sections 48/50 conflict on cross-border flows (see Section III.A).
Cybersecurity & Cybercrime (Arts 24–31)	Partial: Computer Misuse and Cybercrimes Act (CMCA) 2018 criminalises similar offences; Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) provides incident-response capability.	Computer Misuse and Cybercrimes Act (CMCA) lacks explicit Article 25(3) human-rights override. 2025 amendments risk over-criminalisation. Cross-border cooperation is ad hoc rather than treaty-based — the MLA Act 2011 covers no Malabo ratifiers; CMCA Part V cooperation is discretionary without a binding treaty; Cap 43 covers civil judgments only and only 8 countries. Sections 22 and 23 struck down by Court of Appeal (6 March 2026); sections 27 and 48–53 under further review. (See Sections IV.E and IV.F for full MLA analysis.)
Electronic Transactions (Arts 2-7)	Moderate: Kenya Information and Communications Act (KICA) 1998 recognises e-records and signatures as legally valid.	Outdated framework; lacks Artificial Intelligence (AI) and blockchain provisions. Virtual Assets Service Providers Act 2025 (Act No. 20 of 2025, in force 4 November 2025) addresses fintech gaps but is not yet integrated.

Table 1

A. Data Protection and Privacy: The Data Protection Act 2019

The Data Protection Act (DPA) 2019, operationalising Article 31 of the Constitution, mirrors the principles of the European Union (EU) General Data Protection Regulation (GDPR) — lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and integrity/confidentiality — and establishes the independent Office of the Data Protection Commissioner (ODPC).[8] By late 2025, the Office of the Data Protection Commissioner (ODPC) had issued sector-specific guidelines (November 2025), enforcement determinations, and thousands of data-controller registrations.[35]

Gaps include: resource limitations that hinder audits and enforcement; fines (maximum KES 5 million or 1% of annual turnover) that are insufficiently deterrent for global technology companies; broad national security exemptions (section 51) that, in the absence of clear procedural boundaries, could be applied more broadly than intended; and a 90-day statutory investigation limit that hampers complex cross-border investigations.[8] A deeper structural tension identified by an independent legal informatics expert is the conflict between Data Protection Act (DPA) sections 48 and 50. Section 48 provides an adequacy pathway for cross-border data transfers — closely mirroring the Convention's Article 14(6) risk-based approach. However, section 50 empowers the Cabinet Secretary to localise any data of 'strategic interest', giving the government wide discretion to unilaterally block cross-border data flows for reasons of State. This state-centric view of data as a resource to be controlled is in direct tension with the Convention's principle of free data flow, creating what an independent legal expert characterises as a 'fundamental policy choice' that could present a legal paradox upon ratification.[104]

In a landmark practical demonstration of the Data Protection Act (DPA) 2019's data-minimisation principle in action, the Central Bank of Kenya (CBK) in February 2026 granted regulatory approval to Safaricom to implement phone-number masking on M-Pesa peer-to-peer and merchant transactions. Under the new feature, only a truncated version of a sender's number is visible to the recipient (for example, 0718XXXXXX), directly implementing the 'collect only what is necessary' standard under DPA section 25 and the Convention's Article 10 data-minimisation principle. The CBK directed Safaricom to undertake consumer awareness campaigns, monitor feedback, and submit monthly progress reports — institutionalising privacy as a regulatory requirement within Kenya's mobile money infrastructure. Awareness of the Data Protection Act (DPA) remains uneven five years after enactment, but the M-Pesa masking decision, together with incidents such as the Worldcoin biometric data collection controversy, have raised public debate on privacy rights in the digital economy.[37]

B. Cybersecurity and Cybercrimes: The Computer Misuse and Cybercrimes Act Framework

The Computer Misuse and Cybercrimes Act (CMCA) 2018 (amended 2025 by Act No. 17 of 2025) criminalises unauthorised access, cyber-espionage, and child exploitation, aligning broadly with Malabo Articles 24–31.[8] The 2025 amendments expanded powers for content takedowns and enhanced penalties for 'false publications', but faced criticism and partial judicial suspension for posing risks to freedom of expression.[38] The amendments also introduced discretionary takedown powers for the National Computer and Cybercrimes Co-ordination Committee (NC4) without judicial oversight — a significant risk in an increasingly constrained civic space.

Malabo Article 25(3) requires State Parties to ensure that the cyber-security measures they adopt do not infringe on rights guaranteed under the African Charter on Human and Peoples' Rights and other applicable international human rights instruments.

Kenya's Computer Misuse and Cybercrimes Act (CMCA) does not incorporate this explicit safeguard. An independent legal analysis identifies three provisions as specifically failing the Article 25(3) test: section 22 (false publications), section 23 (publication of false information), and section 27 (cyber harassment).

The use of terms such as 'false', 'misleading', and 'detrimentally affects' in these provisions is overly broad — a powerful tool to inadvertently restrict legitimate journalistic and activist activities. This divergence between the Computer Misuse and Cybercrimes Act (CMCA) and the Malabo Convention's Article 25(3) standard underscores the value of a focused legislative review to bring the two frameworks into closer alignment.[104]

Litigation update: Court of Appeal ruling, 6 March 2026. In a significant development directly relevant to this analysis, the Court of Appeal (Justices Patrick Kiage, Aggrey Muchelule, and Weldon Korir) on 6 March 2026 upheld an appeal brought by the Bloggers Association of Kenya (BAKE), ARTICLE 19 Eastern Africa, the Kenya Union of Journalists (KUJ), and the Law Society of Kenya (LSK) and struck down sections 22 and 23 of the Computer Misuse and Cybercrimes Act (CMCA) as unconstitutional. The court found that the provisions criminalising 'false publications' and 'publication of false information' failed the test of constitutional clarity and infringed the freedom of expression guaranteed under Articles 33 and 34 of the Constitution of Kenya. The court confirmed that terms such as 'false', 'misleading', and 'panic' were insufficiently defined, creating unacceptable ambiguity for ordinary citizens. The ruling specifically affirms that reputational harms are properly remedied through civil, not criminal, proceedings.

This ruling is a material development for the arguments in this Brief. It removes the two provisions most cited as incompatible with Malabo Article 25(3) from the operative statute. However, the petitioners noted important limitations: the court declined to strike down the investigation powers in sections 48–53 (which permit judicial-warrant-gated device searches; up to six months of real-time traffic-data collection under section 52(4); and up to nine months of content-data interception under section 53(4)), and section 27 (cyber harassment) was upheld in that ruling, but section 27(1)(b), (c) and (2) remain suspended under conservatory orders issued by High Court Justice Lawrence Mugambi on 22 October 2025 in KHRC & Reuben Kigame v Attorney General pending constitutional review. The Bloggers Association of Kenya (BAKE) and ARTICLE 19 Eastern Africa have indicated they are reviewing further legal avenues, including a potential Supreme Court appeal on the surveillance provisions and section 27. The ruling therefore partially closes the Art 25(3) compliance gap identified in this Brief, while sections 27 and 48–53 continue to require scrutiny against the same standard.

Note: Geoffrey Andare v. Attorney General [2016] eKLR concerned section 29 of the Kenya Information and Communications Act (KICA), which criminalised 'grossly offensive' electronic messages; this provision was struck down for vagueness and infringement of Article 33 of the Constitution. This case is cited for its relevance to the Kenya Information and Communications Act (KICA) framework rather than the Computer Misuse and Cybercrimes Act (CMCA).[39]

C. Electronic Transactions: The Kenya Information and Communications Act Legacy

The Kenya Information and Communications Act (KICA) 1998 (as amended) grants legal validity to electronic records and signatures, aligning broadly with Malabo Article 6 (functional equivalence). Predating the digital boom, it lacks provisions for Artificial Intelligence (AI), blockchain, and smart contracts. The Virtual Assets Service Providers Act, 2025 (Act No. 20 of 2025), effective 4 November 2025, addresses certain fintech gaps but is not yet fully integrated into the broader electronic-transactions framework.

D. Institutional Landscape and Coordination

Overlapping mandates fragment governance: the Office of the Data Protection Commissioner (ODPC) (data protection, under-resourced); the Communications Authority of Kenya (CA)/Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) (threat monitoring); and the National Computer and Cybercrimes Co-ordination Committee (NC4) — whose statutory membership under CMCA section 5(1) comprises the Principal Secretaries for Internal Security (Chair) and ICT, the Attorney-General, the Director of Public Prosecutions, the Chief of the Kenya Defence Forces, the Inspector-General of the National Police Service, the Director-General of the National Intelligence Service, the Director-General of the Communications Authority of Kenya, the Governor of the Central Bank of Kenya, and the Director of the NC4 Secretariat (non-voting) — which has limited transparency in its operations.[40] The Open Government Partnership (OGP) National Action Plan 2023–2027 acknowledges this fragmentation and commits to establishing a Data Governance Council and a comprehensive data capacity improvement programme.[41] Cross-border incident response currently relies largely on informal networks or slow diplomatic channels. Ratification would transform this from ad hoc personal relationships into binding, predictable continental obligations.[120] Ratification would harmonise laws, enable AfCFTA digital flows and affirm leadership.

IV Understanding The Malabo Convention Key Provisions, Strengths & Criticisms

Figure 2 below maps the Convention’s key milestones from its inception through Kenya's Cabinet decision approving a process step towards accession (September 2025) and the March 2026 Court of Appeal ruling, providing the temporal context within which the three substantive pillars analysed in this section should be understood.

Malabo Convention: Timeline of Key Milestones

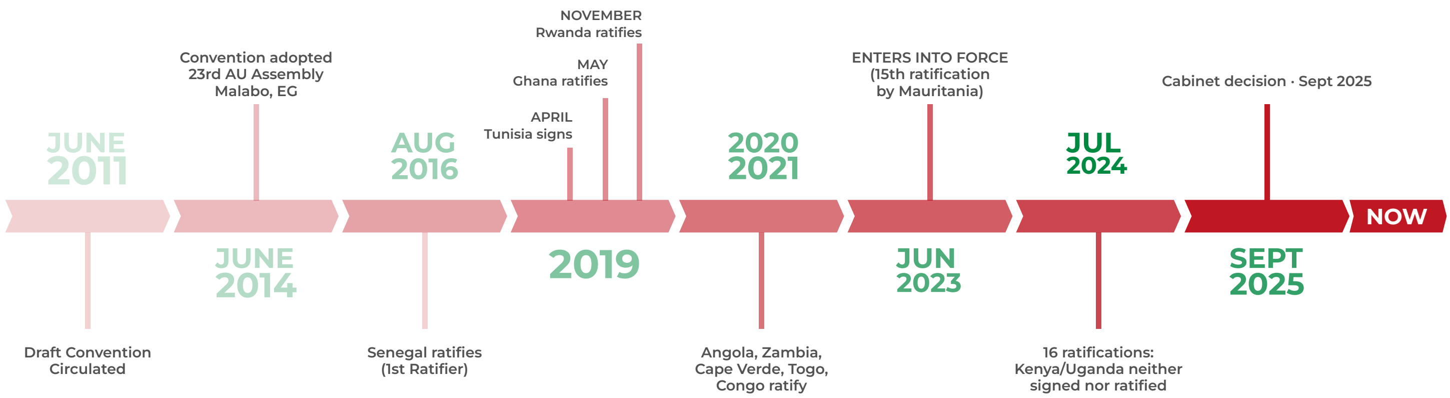


Figure 2: Malabo Convention — Timeline of Key Milestones (2011–2026). Includes Kenya Cabinet Approval (September 2025), CBK–NBR Licence Passporting MoU (March 2026), and Court of Appeal ruling (March 2026) (endnotes 19, 20, 164–168)

A. Personal Data Protection and Privacy (Articles 9–23)

Article 1 (Definitions) defines ‘Personal data’ as ‘any information relating to an identified or identifiable natural person by which this person can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, genetic, mental, cultural, social or economic identity’. Article 14(1) lists racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual life, and health data as sensitive categories whose processing is in principle prohibited. Article 13 enumerates the six principles governing personal data processing: consent and legitimacy; lawfulness and fairness; purpose, relevance and storage; accuracy; transparency; and confidentiality and security. Article 14(1) prohibits the processing of sensitive personal data — covering racial or ethnic origin, political, religious or philosophical opinions, trade union membership, sex life, and health data — except in the limited circumstances enumerated at Article 14(2). Article 11 establishes the national personal data protection authority responsible for ensuring these principles are observed.[19]

Articles 16–19 set out data subjects' rights: the right to information about the processing (Article 16); the right of access to personal data held about them (Article 17); the right to object to the processing on legitimate grounds (Article 18); and the right of rectification, erasure or blocking of inaccurate, incomplete, or unlawfully processed data (Article 19). Article 14(5) regulates automated decision-making, providing that no decision producing legal effects on a data subject may be taken solely on the basis of automated processing. Article 11 mandates the establishment of an independent national personal data protection authority in each State Party. Article 14(6) regulates transborder data flows, requiring that personal data may only be transferred to a non-State Party where the receiving country provides an adequate level of protection.

Article 21 obliges the data controller to implement appropriate technical and organisational security measures. Article 12(2)(m) requires the national protection authority to cooperate with the data protection authorities of other countries, including the African Union, Regional Economic Communities, and third States.

Strengths: Article 10 principles provide a solid foundation for building trust in digital services, with studies estimating a potential 1–2% Gross Domestic Product (GDP) uplift in ratifying states through enhanced data-driven innovation.[47] In Senegal, ratification has strengthened the Commission de Protection des Données Personnelles (CDP), resulting in over 1,000 data-controller registrations and improved compliance.[48]

Criticisms: The Convention lacks mandatory data breach notification timelines (unlike the General Data Protection Regulation (GDPR)'s 72-hour mandate); Article 11 criteria for authority independence are insufficient; and there is limited attention to Artificial Intelligence (AI), biometrics, and algorithmic bias. Independent legal analysis notes that Kenya's Data Protection Act (DPA) uses a significantly broader definition of sensitive personal data than the Convention — including property, marital, and family details — which may work against harmonisation for businesses operating across Africa.[104]

B. Cybersecurity and Cybercrime (Articles 24–31)

Article 24 obliges states to develop national cybersecurity strategies, including Computer Incident Response Teams (CIRTs), public–private partnerships, and capacity building. Article 25 (Legal measures) requires State Parties to adopt legislative and regulatory measures criminalising acts that affect the confidentiality, integrity, availability and survival of ICT systems. The substantive ICT offences — illegal access, illegal interception, data and system interference, misuse of devices, computer-related forgery and fraud, child pornography, and racism / xenophobia via ICT — are codified in Article 29, with adapted sanctions in Article 31. The Convention does not criminalise intellectual-property infringement. Critically, Article 25(3) of the Convention requires State Parties to ensure that the cyber-security measures adopted do not infringe on the rights of citizens guaranteed under the African Charter on Human and Peoples' Rights and other applicable international human rights treaties. Article 26 (National cyber security system) covers cybersecurity culture, public–private partnership, and education and training. Article 27 (National cyber security monitoring structures) covers institutional governance and oversight bodies. Article 28 (International cooperation) requires legislative harmonisation under Article 28(1) and mutual legal assistance under Article 28(2). Procedural investigation powers (subject to judicial oversight under domestic law) are addressed in Article 31(3).

Strengths: Article 24's requirement that every State Party develop a national cybersecurity strategy — including Computer Incident Response Teams (CIRTs), public–private partnerships, and capacity-building — gives the cybersecurity pillar its institutional backbone, and ratifying states have given it concrete effect. Ghana's Cybersecurity Act 2020 (Act 1038), catalysed in part by its Malabo ratification, established a national Computer Incident Response Team (CIRT) and contributed to improved public awareness and public–private collaboration.[61] Article 25(3)'s human-rights safeguard is widely praised as a distinguishing feature positioning the Convention as a model for balanced cybersecurity in Africa.

Criticisms: Terms such as 'cyber-terrorism', 'cyber-harassment', and 'cyber-squatting' in Article 25 are broadly phrased, risking over-criminalisation of legitimate activities such as journalistic investigations or security research. Disproportionate penalties — potentially up to ten years' imprisonment — without sentencing guidelines also raise access-to-justice concerns.

C. Electronic Transactions (Articles 2–7)

Articles 2–7 govern electronic commerce. Article 2 sets the scope of electronic commerce activities, listing exclusions including gambling, legal-representation activities, and notarial functions. Article 6 establishes functional equivalence — information shall not be denied legal effect, validity or enforceability solely because it is in the form of an electronic message. Article 7 sets out the contractual obligations between e-commerce service providers and consumers, including obligations of legal certainty in the formation and performance of electronic contracts. The pillar's main limitation is its outdated focus: it lacks provisions for blockchain, smart contracts, and other emerging technologies. The Kenya Information and Communications Act (KICA) already recognises electronic records and signatures, providing a useful baseline, but requires modernisation.

D. International Cooperation, Final Provisions and Implementation Architecture

Articles 24–31 (Chapter III) address cybersecurity and cybercrime. Article 28 specifically addresses international cooperation, requiring State Parties to provide each other the widest possible mutual legal assistance in cybercrime investigations and prosecutions. Articles 32–38 (Chapter IV) contain the Final Provisions: Article 32 sets the institutional follow-up mechanism, vesting monitoring of the Convention in the Chairperson of the African Union Commission, who reports to the Conference of Heads of State and Government on the Convention's implementation; Article 33 contains the Convention's safeguards clause; Article 34 governs settlement of disputes; Articles 35–38 deal with signature, ratification, entry into force and amendment. As at March 2026, the AU institutional follow-up architecture remains under-resourced; only 16 of 55 AU member states have ratified the Convention as at the date this Brief was prepared (the figure has since risen to 20 — see C.1).[19,20]

Criticisms include insufficient human-rights safeguards in mutual-assistance requests, risking abusive surveillance without adequate due-process protections. A senior official from the Communications Authority of Kenya (CA) notes that current cross-border cooperation relies on informal networks; ratification would provide formal, binding mechanisms for mutual legal assistance.

E. International Cooperation Architecture: The MLA and Foreign Judgments Framework

Kenya possesses three statutory instruments that govern international criminal and judicial cooperation, each relevant to the Malabo Convention's Articles 27 and 29, yet each carrying significant limitations that ratification would directly address.

1. Mutual Legal Assistance Act, No. 36 of 2011

The Mutual Legal Assistance Act (No. 36 of 2011) designates the Office of the Attorney-General as Kenya's Central Authority for processing MLA requests. The Act empowers Kenya to: transmit and receive formal assistance requests; gather, certify, and authenticate evidence; execute search warrants at the request of a foreign state; and arrange for the temporary transfer of persons in custody.[175]

Key gap — no Malabo countries covered: Critically, the Act operates on the principle of mutuality and reciprocity: Kenya is obliged to respond to requests only from states with which it has an applicable international agreement or where reciprocal arrangements exist. This creates a significant structural limitation.

Of Kenya's confirmed Malabo co-ratifiers (Angola, Benin, Cape Verde, Côte d'Ivoire, Congo, Democratic Republic of Congo, Ghana, Guinea, Lesotho, Madagascar, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Sao Tome & Principe, Togo, and Zambia), only Rwanda and Zambia are currently

designated countries under the Foreign Judgments (Reciprocal Enforcement) Act Cap 43. None of the 20 ratifiers are the subject of a dedicated bilateral MLA treaty with Kenya outside of the EAC framework. This means that when a cybercrime originates in — or evidence is located in — Senegal, Ghana, or any other Malabo ratifier, Kenya's current MLA Act provides no automatic or binding mechanism to compel cooperation. Malabo Article 28 (and in particular Article 28(2) on mutual legal assistance) would fill precisely this gap.[176,177]

2. Computer Misuse and Cybercrimes Act, 2018 (Part V) — and the 2025 Amendment

Part V of the CMCA (sections 57–65) creates a parallel international cooperation framework specifically for cybercrime evidence. Section 57 establishes the general principles relating to international cooperation, applied in addition to the Mutual Legal Assistance Act, Cap 75A and the Extradition (Contiguous and Foreign Countries) Act, Cap 76. Sections 59–64 provide detailed procedures for expedited preservation of stored computer data (s.59); expedited disclosure of preserved traffic data (s.60); mutual assistance regarding accessing of stored computer data (s.61); trans-border access to stored computer data with consent or where publicly available (s.62); mutual assistance in real-time collection of traffic data (s.63); and mutual assistance regarding interception of content data (s.64). Section 65 designates the national 24/7 contact point — a requirement that mirrors Budapest Convention Article 35 directly.[7,38]

The CMCA 2025 Amendment (Act No. 17 of 2025, assented to 15 October 2025) significantly strengthened this framework. Key additions include: mandatory obligations on Internet Service Providers (ISPs) and telecommunications operators to preserve and produce user data relevant to investigations when court-ordered; expansion of NC4's authority to block websites promoting illegal activities; and introduction of "critical information infrastructure" (CII) as a defined category requiring annual cyber-risk assessments.[38]

Remaining gap: However, CMCA Part V cooperation remains unilateral and discretionary in the absence of a binding treaty. Requests from non-treaty states are processed through diplomatic channels with no mandatory response obligation — precisely the "informal" arrangement that senior CA officials identified as a core enforcement gap. The CMCA also contains no equivalent to the data-protection safeguard implicit in Malabo Article 28(2) for cross-border requests (requiring that requests must not be used to circumvent data protection safeguards in the requested state).

3. Foreign Judgments (Reciprocal Enforcement) Act, Cap 43

Cap 43 (originally 1984, amended 2018 and revised 2022) provides for recognition and registration of foreign civil judgments in Kenya's High Court where a reciprocal arrangement exists. Kenya currently has reciprocal arrangements with eight countries only: Australia, Malawi, Seychelles, Tanzania, Uganda, Zambia, the United Kingdom, and Rwanda.[176]

The Act is purely civil in scope (it covers money judgments and commercial matters, not criminal or administrative decisions) and is therefore of limited direct relevance to cybercrime enforcement. However, its narrow reach is symptomatic of the deeper problem: Kenya has no binding enforcement architecture with the majority of Malabo's 20 ratifiers. Even Zambia — which is both a Malabo ratifier and a Cap 43 designated country — benefits only from civil judgment recognition, not from criminal MLA obligations.

What Malabo adds: Malabo ratification would, for the first time, create a binding continental framework covering criminal cooperation, digital evidence preservation, and data protection enforcement across all 20 ratifying states — none of which are currently addressable through Cap 43's civil-only reciprocity regime.

4. Kenya Information and Communications Act, Cap 411A (1998, as amended)

KICA, in its amended form, governs the licensing of telecoms and internet services, establishes the Communications Authority of Kenya (CA), and provided the legal basis for the creation of KE-CIRT/CC in 2014. However, KICA was drafted before mobile money, social media, cloud computing, and IoT were significant features of the Kenyan economy. It does not contain provisions on data minimisation, cross-border data transfers, AI, blockchain, virtual asset regulation, or mandatory breach notification.[25,40]

Gap versus Malabo Articles 1–8: KICA's regulatory framework for electronic transactions (Part IV and XII) recognises electronic records and electronic signatures as legally valid, partially satisfying Malabo Article 6 (functional equivalence) and Article 7 (electronic contracts). However, it does not address the consumer-protection obligations in Article 7 to the same depth, which leaves online market participants — particularly SMEs accessing continental markets — without a statutory right of redress equivalent to what Malabo would provide.

The Virtual Assets Service Providers Act, 2025 (Act No. 20 of 2025) took effect on 4 November 2025 (CBK and CMA as dual regulators; licensing not yet operational, pending Regulations), addressing one element of KICA's fintech gap. Modernising KICA — or replacing it with a consolidated Digital Economy Act — is therefore listed as a priority legislative action in the recommendations at Section VIII below.

F. International Cooperation under Chapter III (Article 28) and Final Provisions / Implementation (Articles 32–38): A Detailed Analysis

Article 28 (international cooperation) of the Malabo Convention, supported by the substantive offences and procedural provisions in Articles 29–31 and the institutional follow-up architecture in Articles 32–38, goes significantly further than Kenya's existing bilateral and multilateral frameworks. Each article is analysed below against Kenya's current legal architecture.

Article 28 — International Cooperation in Cybersecurity and Cybercrime

Article 28 requires State Parties to harmonise their cyber-security policies and to engage in international cooperation. Specifically, Article 28(2) provides that State Parties shall implement the necessary mechanisms for mutual legal assistance in cybercrime investigations and prosecutions, ensuring exchange of information consistent with the data-protection regime of each requested State. The Convention does not contain a single 'data-protection override clause' of the kind found in Budapest Convention Article 27; rather, the data-protection requirement is implicit in the Article 28(2) cross-reference back to the Convention's Chapter II personal-data architecture (Articles 8–23).

Kenya gap: Kenya's CMCA Part V (sections 57–65 of Cap 79C) partially implements this architecture, but without a binding treaty framework, the obligation to respond to non-designated states remains discretionary. The MLA Act 2011 fills the general criminal cooperation gap but has no cyber-specific provisions and is limited to designated treaty partners. Malabo Article 28(2) would, on Kenya's ratification, create a binding cyber-specific MLA obligation across all African State Parties — supplementing the rights-safeguard regime in Article 25(3) which neither the MLA Act nor Cap 79C currently provides.

Article 30 — Adapting Substantive Criminal Law to ICT Offences (and the Absence of an Extradition Provision)

Article 30 requires State Parties to adapt their substantive criminal law to cover offences specific to information and communication technologies, ensuring that ICT-enabled conduct is captured by domestic offences in the same way as the equivalent offline conduct. The Convention does not contain a dedicated extradition article; in this respect Malabo differs from the Budapest Convention (which provides for extradition at Article 24) and from the Council of Europe family of cybercrime instruments more generally. Extradition between Malabo State Parties therefore continues to rest on (i) the double-criminality principle as applied through bilateral extradition treaties and (ii) the African Union's general extradition framework.

Kenya gap: Kenya's extradition framework is governed by the Extradition (Contiguous and Foreign Countries) Act (Cap 76) and the Extradition (Commonwealth Countries) Act (Cap 77). Cap 76 operates on the basis of designated countries and applicable treaties; Cap 77 operates within the Commonwealth framework. Of the 16 Malabo ratifiers (now 20 — see Africa Ratification Map at Figure 4), only a minority are Commonwealth members (Ghana, Rwanda, Zambia, Mozambique, Namibia, Mauritius) and none have specific cybercrime extradition arrangements with Kenya. Because Malabo does not contain an extradition provision, ratification of the Convention will not by itself establish a treaty basis for cybercrime extradition. Kenya's extradition framework will continue to rest on Cap 76, Cap 77, and any future bilateral instruments — a gap that the proposed 'Malabo Plus' approach should address through bilateral cybercrime extradition arrangements with Malabo State Parties.

Article 26(4) and Article 31 — Capacity Building (Article 26(4)) and the Adaptation of Sanctions to ICT Offences (Article 31)

Article 26(4) requires State Parties to undertake the necessary measures to develop a culture of cybersecurity, including through awareness-raising, training, and capacity-building of cybersecurity stakeholders. Article 31 obliges State Parties to adapt their sanctions regime to cover offences committed through information and communication technologies.

Read together, these two provisions provide the treaty basis for capacity-building cooperation among State Parties — an obligation that overlays the AfricaCERT framework and AFRIPOL's cybercrime cooperation strategy at continental level.

Kenya opportunity: Kenya participates in AfricaCERT and is a member of the Eastern Africa IGF, but participation is currently discretionary rather than treaty-obligated. As a Malabo State Party, Kenya would have a binding right to request and provide technical assistance — including in developing the CMCA Regulations 2024's cybersecurity operations centres framework — backed by the Convention's Committee of Experts.

Article 32 — Implementation Follow-Up by the Chairperson of the AU Commission

Article 32 establishes the Convention's implementation follow-up mechanism: the Chairperson of the African Union Commission is mandated to monitor the Convention's implementation and report to the Conference of Heads of State and Government. As at March 2026, this reporting mechanism remains under-resourced and has not produced regular public implementation reports. This is a significant governance gap in the Convention itself — not because a Committee of Experts has failed to operationalise (the Convention does not establish one), but because the Chairperson's monitoring function has not been operationally institutionalised. Kenya, upon ratification, should immediately advocate for the establishment of a permanent Convention secretariat (or equivalent) within the AU Commission to support the Article 32 reporting function, with explicit human-rights, AI, and biometrics expertise.

Articles 33–38 — Safeguards, Dispute Settlement, Signature, Entry into Force and Amendment

Article 33 is the Convention's safeguards clause: it preserves non-derogable rights and provides that nothing in the Convention shall be interpreted as authorising any State Party to limit or derogate from rights guaranteed by international law or by the African Charter on Human and Peoples' Rights. Article 34 governs the settlement of disputes between State Parties, providing for negotiation, good offices, and arbitration via the AU. Article 35 addresses signature, ratification or accession. Article 36 governs entry into force. Article 37 governs amendment. Article 38 covers depositary functions and authentic texts. The Convention does not contain a dedicated reservations provision.

Article 34 and Kenya's bilateral MoUs

The Convention does not contain a provision specifically authorising supplementary bilateral digital-trade agreements between State Parties. The CBK–NBR Licence Passporting MoU (11 March 2026) and similar arrangements rest on cooperation between central banks and on the EAC framework rather than on Malabo. The strategic point for Kenya is therefore that Malabo ratification provides the underlying continental rights-and-data architecture against which such bilateral fintech arrangements can be calibrated; it does not, by itself, treaty-formalise those arrangements.[67,168]

Country-by-Country: Mutual Legal Assistance and Enforcement Cooperation Frameworks

The table below maps each comparator country's MLA and enforcement cooperation architecture against Malabo's Article 28 international-cooperation requirements (covering harmonisation under Article 28(1), mutual legal assistance under Article 28(2), and exchange of information including CERT/CSIRT cooperation).

Country Mutual Legal Assistance and Enforcement Cooperation Frameworks vs Malabo

COUNTRY STATUS	MLA & ENFORCEMENT COOPERATION FRAMEWORK	IMPLICATION FOR KENYA MALABO RATIFICATION
SENEGAL Malabo ratifier (August 2016) Budapest Convention Party (2016)	Senegal's data protection authority(CDP) and cybercrime law (Law No. 2016-29) implement Malabo obligations domestically. As one of only five African states party to BOTH Malabo and the Budapest Convention, Senegal's law enforcement agencies have access to two binding cooperation frameworks simultaneously. The CDP has MLA capacity for transborder data flow disputes. Senegal's national cybersecurity strategy explicitly commits to bilateral and multilateral law enforcement cooperation.	Strong dual-framework architecture. Kenya has no equivalent bilateral arrangement with Senegal; Malabo ratification would create the first binding basis for cybercrime cooperation and data protection enforcement between the two countries.
GHANA Malabo ratifier (May 2019) Budapest Convention Party (ratified April 2019)	Ghana's Cybersecurity Act 2020 (Act 1038) requires the Cyber Security Authority to designate and maintain a 24/7 contact point to tackle cybercrime, satisfying Budapest Convention Article 35. The Cyber Security Authority (CSA) has received EU/Council of Europe GLACY+ capacity-building support on MLA procedures for cybercrime and electronic evidence. Ghana's 2025 Cybersecurity Amendment Bill adds extradition provisions. Ghana is a Party to the ECOWAS framework and holds bilateral MLA treaties with multiple European and North American states.	Strongest MLA architecture of all five comparators. Kenya lacks an equivalent bilateral arrangement with Ghana. Malabo ratification would create the binding basis for cybercrime cooperation. Ghana demonstrates that Malabo and Budapest ratification are complementary, not alternatives.
RWANDA Malabo ratifier (November 2019) Not a Budapest Convention party	Rwanda's Law No. 60/2018 on Prevention and Punishment of Cyber Crimes addresses substantive offences and partial procedural provisions but requires further regulation on monitoring and interception. Rwanda lacks a standalone MLA Act; cooperation relies on the cybercrime law and bilateral arrangements. Kenya and Rwanda have an existing Cap 43 reciprocal enforcement arrangement (civil judgments only) and the CBK-NBR Licence Passporting MoU (11 March 2026). Rwanda is a member of the EAC framework and INTERPOL. The DPO-NCSA co-location model means a single authority handles both data protection MLA requests and cybercrime cooperation.	Moderate cooperation framework. The existing Cap 43 arrangement covers civil judgments only and does not extend to cybercrime. Malabo ratification by Kenya would create the first binding criminal cooperation framework between the two countries, and formalise arrangements such as the March 2026 CBK-NBR MoU under treaty law.
UGANDA Neither signed nor ratified Malabo Not a Budapest Convention party	Uganda's Computer Misuse Act 2011 (amended 2022) does not contain comprehensive MLA provisions for cybercrime. The Data Protection and Privacy Act 2019 places the authority (PDPO) under NITA-U, which lacks enforcement cooperation mechanisms with foreign data protection authorities. Uganda is a Cap 43 designated country with Kenya (civil judgments only). Without Malabo ratification: (a) no binding data protection cooperation with Kenya exists under any continental framework; (b) no cybercrime-specific MLA obligations apply; (c) cross-border incidents rely on INTERPOL and ad hoc diplomatic channels.	Cooperation gap. Cross-border cyber incidents between Kenya and Uganda currently rely on informal channels and bilateral diplomacy. Malabo ratification by both countries would establish the formal, binding mechanism both jurisdictions need for the growing volume of shared digital trade and cross-border data flows.

COUNTRY STATUS	MLA & ENFORCEMENT COOPERATION FRAMEWORK	IMPLICATION FOR KENYA MALABO RATIFICATION
TUNISIA Signed Malabo (April 2019) Not yet ratified; not a Budapest Party	Decree-Law No. 2023-17 on Cybersecurity establishes CERT-TUN and references international cooperation, but in the absence of Budapest or Malabo ratification, Tunisia has no binding multilateral cybercrime MLA framework. Organic Law No. 2004-63 (data protection) contains no cross-border enforcement mechanism. Tunisia's cybercrime cooperation relies entirely on bilateral and informal arrangements, with no treaty-based obligation to respond to requests from any African state including Kenya.	Cooperation and rights-balance gap. Tunisia's non-ratification leaves its cybercrime cooperation in a bilateral, ad hoc state. Malabo ratification would strengthen Tunisia's international cooperation framework and provide the Article 25(3) standard that regional organisations have called for. Tunisia's strong commercial innovation environment (Startup Act: 1,040+ labelled startups) would benefit from the continental trust architecture that Malabo provides.

Table 2: Country Mutual Legal Assistance and Enforcement Cooperation Frameworks vs Malabo

The MLA Gap and What Malabo Closes

The analysis above reveals a structural asymmetry at the heart of Kenya's current international cooperation architecture. Kenya has strong domestic cybercrime and data protection laws (CMCA 2018/2025, DPA 2019, KICA Cap 411A) and a functional general MLA framework (MLA Act 2011, Cap 76, Cap 77). However, these instruments collectively fail to create binding, cyber-specific, rights-respecting cooperation obligations with any of the 20 Malabo ratifiers — the very states most likely to be the origin or destination of cross-border cyber incidents affecting Kenya.

This gap has four concrete consequences. First, when a ransomware attack originates in a Malabo ratifier state, Kenya's CMCA section 69 contact point can request cooperation but has no binding right to receive it; the request is routed through diplomatic channels at the discretion of the receiving state. Second, electronic evidence located in Senegal, Ghana, or Rwanda cannot be compelled through any existing treaty mechanism — only through informal INTERPOL channels or the bilateral MLA Act, which covers none of these countries. Third, a data subject whose personal data has been unlawfully processed by a company in another African state has no continental enforcement mechanism; the ODPC can investigate but cannot compel a foreign DPA to act. Fourth, the Cap 43 civil judgments regime covers only Rwanda among all Malabo ratifiers, and covers civil matters only — it cannot support the criminal enforcement cooperation that cybercrime requires.

The case for Malabo as MLA architecture: Malabo ratification closes all four of these gaps simultaneously through a single treaty instrument, binding on all 20 current and all future State Parties. No bilateral treaty negotiation — which takes years and is limited to individual country pairs — can achieve the same breadth of coverage.

Comparative Analysis: Approaches to Digital Governance in Africa

This section analyses digital governance frameworks in five comparator states — Senegal, Ghana, Rwanda (all ratifiers), and Uganda and Tunisia (both non-ratifiers or signatories with ratification pending) — drawing strategic lessons for Kenya. Ghana and Rwanda are included as non-ReCIPE Project Countries due to the substantive lessons their experience offers. A consolidated cross-country overview appears in Table 8 at the close of this section.

Figure 3 provides the quantitative baseline for this comparative analysis, tracing ITU Global Cybersecurity Index scores across all five GCI editions (2014–2024) for all six comparator countries.

ITU Global Cybersecurity Index - Multi-Edition Trajectory 2014-2024
Six Malabo comparator countries across all five GCI edition
(GCI 2014 & 2017 normalised x100 for visual comparison)

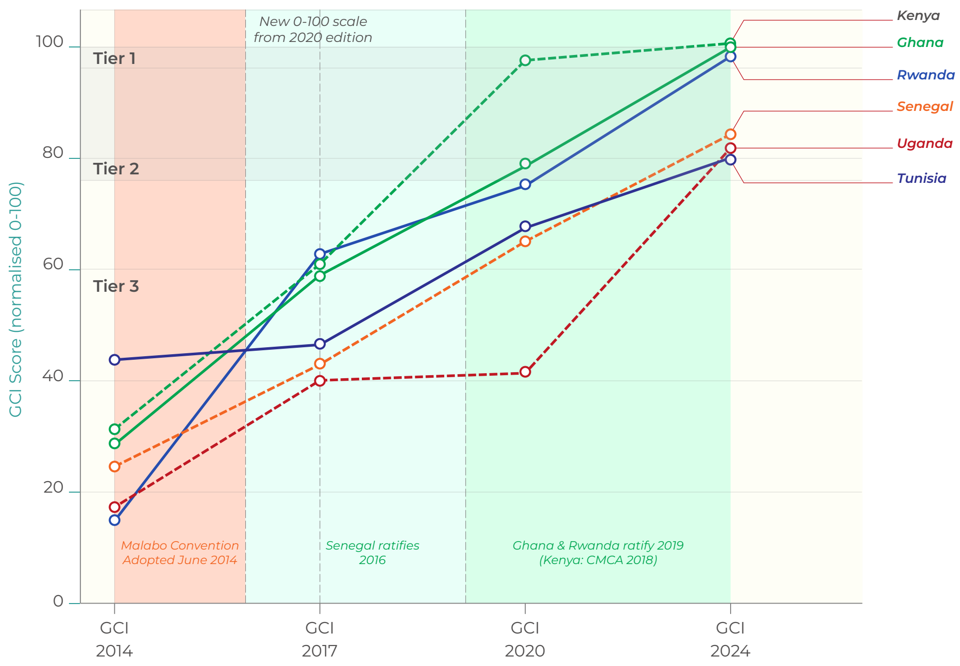


Figure 3: ITU Global Cybersecurity Index — Multi-Edition Trajectory 2014–2024. All five GCI editions across six Malabo comparator countries (GCI 2014 and 2017 normalised ×100; methodology changed in 2020). Sources: ITU GCI 2014, 2017, 2020, 2024; bizcommunity.africa (2017); BOCRA (2020). Endnotes 178, 184, 185.

Figure 3 tracks the ITU Global Cybersecurity Index (GCI) for all six comparator countries across the five editions published between 2014 and 2024 (the 2014 and 2017 scores are normalised to a 0–100 scale for comparability with the post-2020 methodology). Two patterns stand out: the early Malabo ratifiers, Ghana and Rwanda, recorded the steepest sustained gains and overtook Kenya despite starting from lower 2014 baselines; and all three ratifiers now sit in the Index's top tier. The trajectory suggests the Convention's framework provides structural acceleration in cybersecurity governance beyond what organic national development alone delivers.

Malabo Convention Ratification Status (February 2026 - Official AU Record)

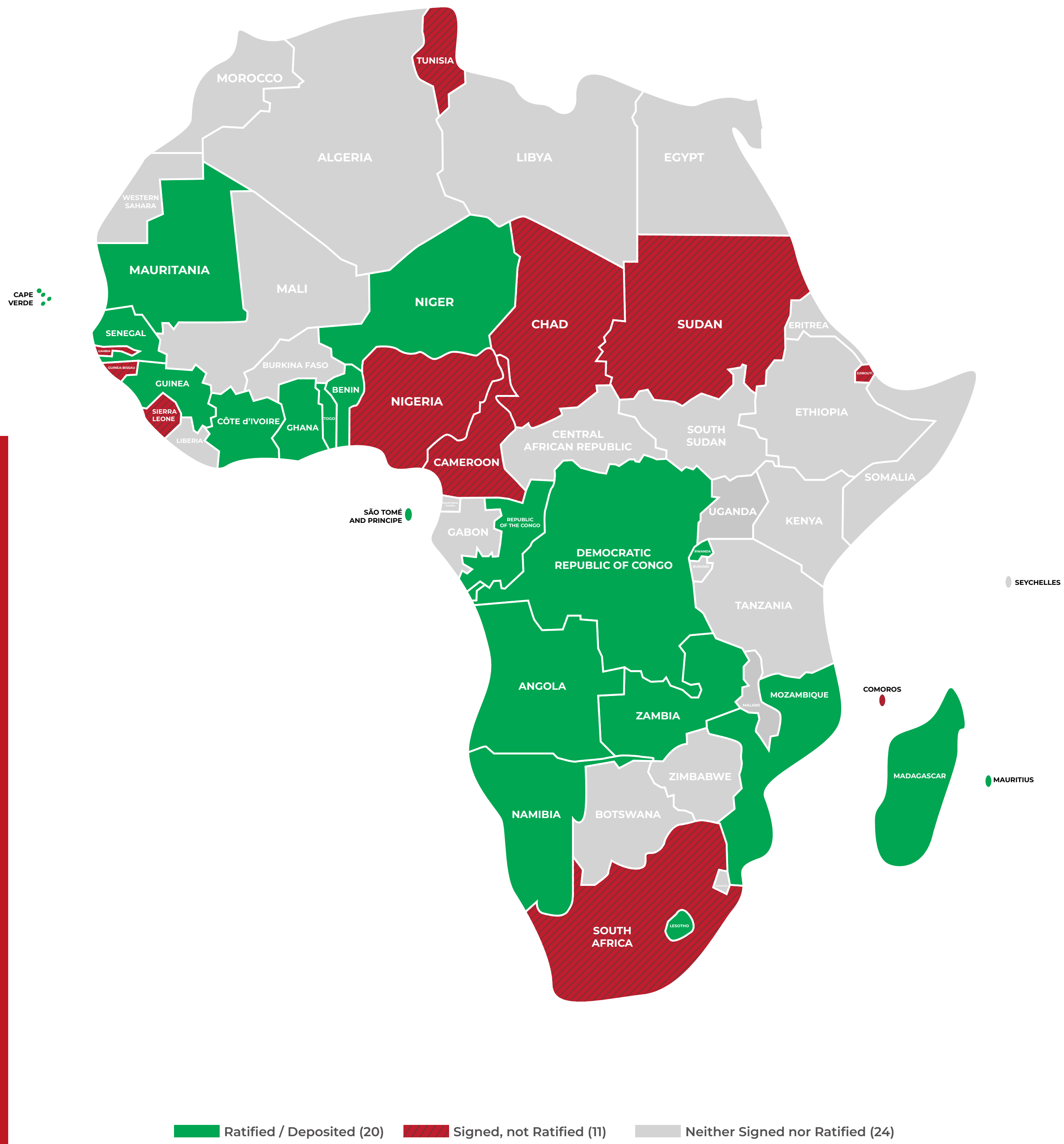


Figure 4: Malabo Convention Ratification Status (February 2026). Twenty AU member states have ratified. Kenya's Cabinet approved the process towards accession in September 2025; Kenya has neither signed nor ratified as at the AU Status List date. Source: AU Status List (02/02/2026).

A. Senegal: Leading the Way in Malabo Ratification and Implementation

Senegal ratified the Malabo Convention in August 2016, one of the first African Union (AU) member states to do so. Under the current government's 'Senegal Vision 2050' agenda, a strategic roadmap known as the New Deal Technologique (NDT) — launched in February 2025 — aims to position Senegal as a continental technological hub fully aligned with the Convention's three pillars.[51] The New Deal Technologique (NDT) is not legislation but a strategic vision. A partnership agreement signed with the Bill & Melinda Gates Foundation in September 2025 (valued at approximately US$10 million) will support a universal digital identity, an Artificial Intelligence (AI) hub for health and agriculture, and a Delivery Unit for transparency.[52]

1. Personal Data Protection

Senegal's data protection regime is anchored in Law No. 2008-12 of 25 January 2008, which established the Commission de Protection des Données Personnelles (CDP) as the independent national personal data protection authority required by Malabo Article 11.[53] The Commission de Protection des Données Personnelles (CDP) publishes quarterly reports (avis trimestriel) detailing authorisations, complaint handling, formal notices, and sanctions. Over 1,000 data-controller registrations have been achieved as of mid-2025.[48]

2. Cybersecurity and Cybercrime

Law No. 2016-29 of 8 November 2016 amended the Senegalese Penal Code to incorporate cybercrime provisions of Malabo Articles 25 and 29 directly into the primary criminal framework — cybercrime is therefore no longer a standalone text.[55] The Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI) is the state's principal entity for information systems security. Within it, the Centre National Opérationnel de Cybersécurité (CNOC) provides continuous monitoring and management of cyber risks.[56]

3. Electronic Transactions

Law No. 2008-08 of 25 January 2008 on Electronic Transactions grants legal validity to digital contracts and signatures.[57] The Autorité de Régulation des Télécommunications et des Postes (ARTP), established as an independent administrative body with financial and administrative autonomy, regulates the telecommunications and postal sectors.[57]

SECTOR	KEY LEGISLATION	ALIGNMENT WITH MALABO	KEY HUMAN RIGHTS SAFEGUARDS
Data Protection	Law No. 2008-12; Commission de Protection des Données Personnelles (CDP)	High: consent and minimisation enforced; CDP publishes quarterly sanction reports; 1,000+ registrations.	CDP independence ensures accountability; rights to access and rectification active.
Cybersecurity	Law No. 2016-29 (Penal Code); New Deal Technologique (NDT) 2025; Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI) & Centre National Opérationnel de Cybersécurité (CNOC)	Strong: cybercrimes in Penal Code; DCSSI leads national strategy (Malabo Arts 24–31).	Focus on 'Digital Trust' implies user protection; however, surveillance provisions draw civil society scrutiny.

Table 3: Comparative Analysis — Senegal

SECTOR	KEY LEGISLATION	ALIGNMENT WITH MALABO	KEY HUMAN RIGHTS SAFEGUARDS
Electronic Transactions	Law No. 2008-08; Autorité de Régulation des Télécommunications et des Postes (ARTP)	Strong: e-signatures and contracts valid; ARTP ensures secure infrastructure.	ARTP autonomy insulates the sector from undue political interference.

Table 3: Comparative Analysis — Senegal

B. Ghana: A Robust Data Protection Framework and Cybersecurity Focus

Ghana signed the Malabo Convention in 2017 and ratified it in May 2019 and has since domesticated its principles through targeted legislation. The Information and Communication Technology (ICT) sector grew by 13.1% in Q1 2025, significantly outperforming national Gross Domestic Product (GDP) growth.[58]

1. Personal Data Protection

Ghana's data protection regime is governed by the Data Protection Act, 2012 (Act 843), which established the Data Protection Commission (DPC).[59] The Data Protection Commission (DPC) registered over 1,200 data controllers and conducted more than 150 audits annually as of mid-2025.[60] The Data Protection Commission (DPC) operates as a statutory body under the Ministry of Communications and Digitalisation — a hybrid independence model that, while compliant with Malabo's text, mirrors oversight challenges seen in Kenya. Both the Kenyan Office of the Data Protection Commissioner (ODPC) and Ghana's Data Protection Commission (DPC) sit in this hybrid zone: independent in mandate, but constrained in their relationship to the executive.

2. Cybersecurity and Cybercrime

The Cybersecurity Act, 2020 (Act 1038) established the Cyber Security Authority (CSA) and mandated the National Computer Emergency Response Team (CERT-GH).[61] A total ban on unlicensed cybersecurity service providers and professionals took effect 1 January 2024. By mid-2024, the Cyber Security Authority (CSA) had registered 1,353 professionals and 226 providers.[62] The Cybersecurity (Amendment) Bill, 2025 proposes direct prosecutorial powers for the Cyber Security Authority (CSA), an explicit Artificial Intelligence (AI), blockchain, and quantum computing mandate, and operationalisation of the Cybersecurity Fund.[63,64]

3. Electronic Transactions

The Electronic Transactions Act, 2008 (Act 772) provides the legal foundation for digital commerce. As the 2008 law pre-dates Malabo, it lacks specific provisions for smart contracts and automated agreements.

4. Gender Disparities and the Malabo Gap

A significant finding in the Ghanaian context is the absence of explicit gender provisions in the Malabo Convention — the text is largely gender-neutral. The Cybersecurity Act 2020 actively addresses this by criminalising the non-consensual sharing of intimate images (Section 67). The 2025 Amendment Bill further introduces a statutory function to promote the online protection of women, children, the elderly, and persons with disabilities, directly addressing a policy gap in the original Malabo text. This dimension — absent from all other comparator countries — should be adopted in Kenya's ratification instrument.

SECTOR	KEY LEGISLATION	ALIGNMENT WITH MALABO	KEY HUMAN RIGHTS SAFEGUARDS
Data Protection	Data Protection Act 2012 (Act 843); Data Protection Commission (DPC)	High: 1,200+ controllers; 150+ audits/yr; mirrors Malabo Arts 9–23.	Hybrid independence: statutory body under Ministry; complies with Malabo Article 11 but lacks General Data Protection Regulation (GDPR)-level insulation.
Cybersecurity	Cybersecurity Act 2020 (Act 1038); Amendment Bill 2025; Cyber Security Authority (CSA)	Strong: criminalises core offences; establishes National Computer Emergency Response Team (CERT-GH); mandatory licensing (2024).	Gender response: 2025 Bill explicitly mandates protection of women online, filling a Malabo gap.
Electronic Transactions	Electronic Transactions Act 2008 (Act 772)	Moderate: predates Malabo; aligns with functional equivalence principles.	Facilitates digital trade but lacks updates for Artificial Intelligence (AI)/automated contracts.

Table 4: Comparative Analysis — Ghana

C. Rwanda: Progressive Digital Transformation with Integrated Policy

Rwanda ratified the Malabo Convention in 2019 and has integrated its principles into a cohesive policy framework supporting the 'Vision 2050' agenda. The Information and Communication Technology (ICT) sector expanded by 19% in Q1 2025, significantly outpacing national Gross Domestic Product (GDP) growth of 7.8%.[66]

1. Personal Data Protection

Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy establishes the Data Protection Office (DPO) within the National Cyber Security Authority (NCSA).[67] The law grants data subjects robust rights, including data portability. As of 2025, the Data Protection Office (DPO) requires all entities outside Rwanda processing Rwandan residents' data to designate a local representative — mirroring the extraterritorial reach of the European Union (EU) General Data Protection Regulation (GDPR).[69]

2. Cybersecurity and Cybercrime

The National Cybersecurity Strategy 2024–2029 outlines seven objectives, including protection of Critical Information Infrastructure, building a sovereign cybersecurity industry, and embedding a cybersecurity culture in the national curriculum.[71] Rwanda actively participates in regional cyber diplomacy, with the strategy explicitly mandating the development of 'cyber-diplomacy capabilities' aligned with Malabo's Article 28 international-cooperation framework and the cybersecurity-culture obligations at Article 26.

3. Electronic Transactions

On 25 February 2025, the National Bank of Rwanda (NBR) and the Bank of Ghana (BoG) signed Africa's first 'Fintech Licence Passporting' agreement, allowing fintech companies licensed in one country to operate in the other with minimal additional regulatory hurdles — directly operationalising African Continental Free Trade Area (AfCFTA) digital-trade protocols.[72,73] Rwanda's National Artificial Intelligence (AI) Policy (approved by Cabinet in April 2023) focuses on ethical guardrails and positions Rwanda as an 'AI Lab' for Africa.

4. The Governance Dualism Challenge

Rwanda’s decision to integrate the Data Protection Office (DPO) within the National Cyber Security Authority (NCSA) reflects a deliberate policy choice to treat data protection and cybersecurity as complementary disciplines rather than competing concerns. This integrated model enables a unified institutional response to threats that are inherently cross-cutting: a data breach, for instance, is simultaneously a cybersecurity incident and a data protection violation requiring both technical response and regulatory action. Rwanda’s approach mirrors the co-located models seen in some of Europe’s most effective digital governance jurisdictions. The NCSA’s institutional capacity, technical expertise, and established operational protocols provide the DPO with enforcement infrastructure that a standalone privacy authority would take years to build. The 2024–2029 National Cybersecurity Strategy’s explicit commitment to ‘Digital Trust’ as a strategic objective reflects an understanding that citizens’ trust in digital systems depends equally on cybersecurity resilience and data protection guarantees. Civil society should monitor for independence in practice, but the structural integration is a governance innovation worth studying rather than dismissing.

SECTOR	KEY LEGISLATION	ALIGNMENT WITH MALABO	KEY HUMAN RIGHTS & STRATEGIC NOTES
Data Protection	Law No. 058/2021; Data Protection Office (DPO) under National Cyber Security Authority (NCSA)	High: mandatory registration; local representative rules (2025) enforce Malabo Convention.	Integrated governance model: DPO co-located within the National Cyber Security Authority (NCSA) enables unified response to data breaches as both cybersecurity incidents and privacy violations. Reflects Rwanda's 'Digital Trust' strategy; monitors for operational independence.
Cybersecurity	Cyber Crimes Law (2018); National Cybersecurity Strategy 2024–2029	Strong: strategy focuses on 'Cyber Resilience' and 'Digital Trust' (Malabo Art 24).	Surveillance: cybercrime laws curb 'false information', often targeting dissent; tension between security goals and Article 25(3) rights safeguards.
Electronic Transactions	Law Governing Payment System (2021); National Artificial Intelligence (AI) Policy (2023)	Advanced: Fintech 'Licence Passporting' with Ghana (February 2025) sets a continental benchmark.	Fintech integration is a primary economic driver; strong regulatory clarity for investors.

Table 5: Comparative Analysis — Rwanda

D. Uganda: Navigating Data Protection and Cybercrime Legislation

Uganda has neither signed nor ratified the Malabo Convention as at March 2026. Gross Domestic Product (GDP) expanded by 6.3% in the 2024/2025 fiscal year, with the services sector — underpinned by Information and Communication Technology (ICT) — serving as a primary growth engine.[75] The Global Innovation Index 2025 ranks Uganda 4th among low-income economies, highlighting a resilient though constrained innovation ecosystem.[76]

1. Personal Data Protection

In a landmark decision on 18 July 2025, the Personal Data Protection Office (PDPO) ruled against Google LLC on a complaint by four Ugandan citizens (Complaint No. 08/11/24/6683), finding the company in breach of the Data Protection and Privacy Act for operating without registration as a data controller and data collector and for failing to demonstrate adequate safeguards for the cross-border transfer of Ugandan data subjects' personal data; the PDPO ordered Google to register within 30 days, affirming the Act's extraterritorial application to all entities processing Ugandan citizens' data regardless of where they are based and operationalising Malabo's sovereignty principle.[78] Unlike Kenya's Office of the Data Protection Commissioner (ODPC) — which, while established as a constitutionally mandated independent office, remains dependent for its budget on the National Treasury, channelled through the State Department responsible for ICT, and operates under a hybrid-independence model —

2. Cybersecurity and Cybercrime

The Computer Misuse Act, 2011 (amended 2022) and the National Cybersecurity Strategy 2022–2026 address cybercrime and incident response.[79] In January 2023, the Constitutional Court nullified Section 25 ('offensive communication') as unconstitutional — a significant digital-rights victory aligning Uganda with Malabo's Article 25(3) safeguards.[80] However, the 2022 amendments introduced broadly defined offences including 'unauthorised sharing of information' and 'misuse of social media', reportedly used in 2024–2025 to arrest activists protesting the East African Crude Oil Pipeline (EACOP).[81]

3. Electronic Transactions and Digital Integration

The Electronic Transactions Act, 2011 provides the baseline for e-commerce. The 2025 Tax Amendment Bills mandate the linkage of Business Registration Numbers with digital National IDs and tax systems for all entities — enhancing the trust environment for e-transactions (Malabo Article 8) while raising exclusion concerns for unregistered populations and informal sector workers, estimated at 65% of the workforce.[82]

SECTOR	KEY LEGISLATION	ALIGNMENT WITH MALABO	KEY HUMAN RIGHTS & STRATEGIC NOTES
Data Protection	Data Protection and Privacy Act 2019; Personal Data Protection Office (PDPO) under National Information Technology Authority—Uganda (NITA-U)	Moderate: high alignment in text; Google 2025 ruling proves strong extraterritorial enforcement.	Structural flaw: Personal Data Protection Office (PDPO) sits under National Information Technology Authority—Uganda (NITA-U) (government agency), unlike Kenya's hybrid-independence model.

Table 6: Comparative Analysis — Uganda

SECTOR	KEY LEGISLATION	ALIGNMENT WITH MALABO	KEY HUMAN RIGHTS & STRATEGIC NOTES
Cybersecurity	Computer Misuse Act (2011, amended 2022); National Cybersecurity Strategy 2022–2026	Partial: strategy aligns with Malabo Art 24; criminalisation covers core offences.	Human rights concern: 2022 amendments introduced broadly-drafted speech offences ('misuse of social media') after courts struck down old ones; used against dissenters.
Electronic Transactions	Electronic Transactions Act 2011; Tax Amendment Bills 2025	High: legal recognition of e-records aligns with Art 1.	Surveillance risk: 2025 tax amendments aggressively link digital ID to all economic activity.

Table 6: Comparative Analysis — Uganda

E. Tunisia: A Pioneering Approach in the North African Context

Tunisia signed the Malabo Convention in 2019 but has not ratified it as at March 2026. The digital sector contributes approximately 7.5% to Gross Domestic Product (GDP) in 2025 with an annual growth rate of approximately 8%.[84] However, a stark duality characterises digital governance: a vibrant innovation ecosystem coexisting with an increasingly restrictive cybersecurity regime.[83]

1. Personal Data Protection

Tunisia was one of the first African nations to constitutionalise privacy (2014, now Article 24 of the 2022 Constitution) and enact a data protection law (Organic Law No. 2004-63).[84] The National Authority for the Protection of Personal Data (INPDP) oversees registration, audits, and enforcement. A comprehensive draft Code of Digital Rights — intended to align Tunisia with General Data Protection Regulation (GDPR) standards — has been pending parliamentary approval for several years. The National Authority for the Protection of Personal Data (INPDP) lacks the statutory power to impose significant financial penalties, diverging from the effective-sanctioning-power requirement implicit in Malabo Article 12 (which sets out the duties and powers of the national protection authority, including, at Article 12(4), the power to investigate, formally caution, and sanction).[85]

2. Cybersecurity: The Rights Concern

Decree-Law No. 2023-17 of March 2023 established the National Cybersecurity Agency (ANCS), aligning technically with the institutional-framework obligations at Malabo Article 27(2) and the cybersecurity-culture obligations at Article 26.[86] However, Decree-Law No. 2022-54 of September 2022 imposes up to five years' imprisonment for 'false news' and 'rumours'. In 2024 and 2025, this provision has been applied in cases involving journalists, legal practitioners, and commentators, raising concerns from press freedom organisations regarding its compatibility with international human rights standards.[87,88] This experience highlights why the rights-balancing standard in Malabo Article 25(3) provides valuable guidance for all jurisdictions navigating similar legislative design questions. Tunisia's experience provides a clear lesson for Kenya: aligning domestic digital legislation with a binding regional standard provides ongoing guidance that helps legislators and courts calibrate protections appropriately as technology and society evolve.[83]

3. Electronic Transactions and the Innovation Balance

The Startup Act (Law No. 2018-20) has labelled over 1,040 startups, positioning Tunisia as the 5th largest startup hub in the Middle East and North Africa (MENA) region.[89] This commercial vitality demonstrates that economic innovation can coexist with, though ultimately be undermined by, contracting civic digital freedoms.

SECTOR	KEY LEGISLATION	ALIGNMENT WITH MALABO	KEY HUMAN RIGHTS & STRATEGIC NOTES
Data Protection	Organic Law No. 2004-63; National Authority for the Protection of Personal Data (INPDP)	Partial: predates Malabo; lacks modern definitions and deterrent penalties.	Adequacy gap: failure to update the 2004 law hinders full data integration with European Union (EU) and African Union (AU) partners.
Cybersecurity	Decree-Law No. 2022-54 (Cybercrime); Decree-Law No. 2023-17 (National Cybersecurity Agency (ANCS))	Divergent: technical alignment (National Cybersecurity Agency (ANCS)) overshadowed by broadly-drafted laws (Decree 54) that have raised human rights concerns.	Human rights concern: the 'false news' provision has been applied to prosecute journalists and critics, raising concerns about compatibility with Malabo Art 25(3).
Electronic Transactions	Law No. 2000-83 (E-Commerce); Startup Act 2018	High: strong legal certainty for business; Startup Act is a regional best practice.	The 'Innovation Paradox': startups thrive under special laws while citizens face pressures on digital rights. Malabo's Article 25(3) is designed to guide this balance constructively.

Table 7: Comparative Analysis — Tunisia

F. Strategic Lessons for Kenya: Synthesising Comparative Insights

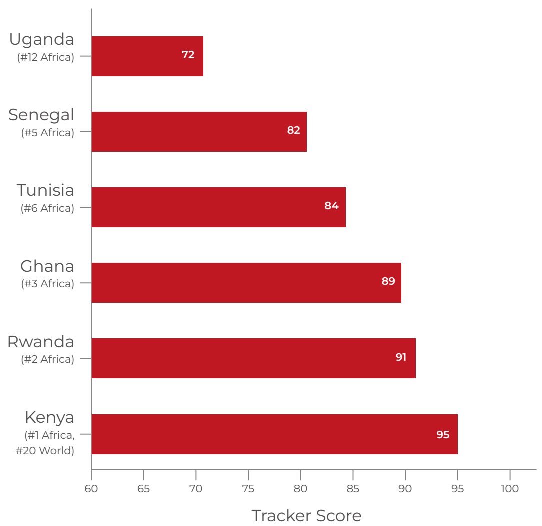
COUNTRY	National Cyber Strategy (ART 24)	CERT/CIRT Established	Core Offences Criminalised (Art 29)	Art 25(3) Human Rights Safeguard	Mutual Assistance & Cooperation (Art 28)
SENEGAL (Ratified)	Strong	Strong	Strong	Strong	Partial
GHANA (Ratified)	Strong	Strong	Partial	Partial	Partial
RWANDA (Ratified)	Strong	Strong	Strong	Partial	Strong
UGANDA (Not Signed)	Partial	Partial	Partial	Divergent	Partial
TUNISIA (Signed)	Partial	Divergent	Strong	Partial	Divergent
KENYA (Cabinet approved process step towards accession)	Partial	Strong	Partial	Partial	Partial

Figure 5: Country Compliance Scorecard — Traffic Light Matrix. Green = strong alignment; Amber = partial/gaps; Red = divergent/risk; Grey = not applicable (endnotes 51, 57, 63, 69, 80)

1. The Institutional Independence Lesson: Financial Autonomy as the Bedrock of Enforcement

The regulatory performance data provides empirical grounding for this strategic lesson. Figure 6 maps Kenya's position on the ITU ICT Regulatory Tracker 2024 against the data-protection coverage of Malabo and non-Malabo states, demonstrating that regulatory leadership and Malabo ratification are mutually reinforcing, not competing, governance commitments.[178,182]

ITU ICT Regulatory Tracker 2024 (Africa Leaders)



Africa Data Protection & Malabo Coverage (Au Member States, 2025-25)

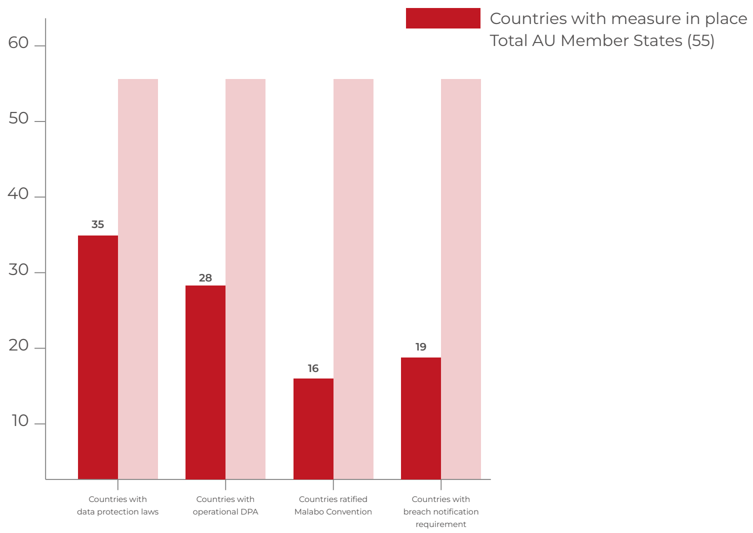


Figure 6: ITU ICT Regulatory Tracker 2024 and Africa Data Protection Coverage. Sources: ITU Regulatory Tracker 2024 (Kenya #1 Africa, #20 globally); UNCTAD Data Protection Report 2024; AU Malabo Status List (endnotes 178, 182)

The experiences of Senegal and Ghana reveal that statutory independence is illusory without financial autonomy. Kenya's Office of the Data Protection Commissioner (ODPC) remains dependent for its operational budget on the National Treasury, channelled through the State Department responsible for ICT, limiting its capacity. Senegal's Commission de Protection des Données Personnelles (CDP) achieves compliance rates exceeding 80% among major data processors because it exercises rigorous enforcement powers that compel registration.[48] Ghana offers a blueprint for fiscal sustainability: the 2024 licensing regime for cybersecurity professionals creates a self-sustaining, non-exchequer revenue stream, insulating the Cyber Security Authority (CSA) from political budgetary fluctuations.[62] Ratification should be accompanied by amendments to the Data Protection Regulations to allow the Office of the Data Protection Commissioner (ODPC) to retain a percentage of administrative fines and registration fees, creating a 'Data Protection Fund' modelled on the Ghanaian approach.

Figure 7: ICT Sector Growth, Cybersecurity & Digital Economy — Malabo Ratifiers vs Non-Ratifiers. Three-panel comparison using ITU GCI 2024; World Bank WDI 2024; GSMA Mobile Economy Africa 2025 (endnotes 178, 179, 180, 187)

2. The Integrated Policy Lesson: Cybersecurity as a Trade Enabler

Rwanda distinguishes itself by treating cybersecurity not merely as a national security imperative but as a fundamental enabler of international trade. The Rwanda–Ghana Fintech Licence Passporting Agreement of February 2025 is the most tangible example of Malabo's African Continental Free Trade Area (AfCFTA) integration in action.[72] Kenya should frame the Malabo Convention to the private sector not as a compliance burden but as a commercial necessity — a 'VIP ticket' for Kenyan fintechs to access the continental Digital Single Market under the African Continental Free Trade Area (AfCFTA). As a senior official from the Communications Authority of Kenya (CA) observed, Malabo is the 'how' to the African Continental Free Trade Area (AfCFTA)'s 'what'.[120]

3. The Rights-Based Lesson: A Continental Standard Strengthens Domestic Frameworks

The comparative record shows that a continental rights-based standard benefits all stakeholders — governments, businesses, and citizens alike. Ratifying the Malabo Convention anchors Kenya to Article 25(3), which requires that cybersecurity measures protect, rather than restrict, fundamental freedoms including freedom of expression and the right to a fair hearing. This standard is not a constraint on government authority; it is a confidence signal to investors, trading partners, and the international community that Kenya's digital governance meets the highest continental benchmark.[80]

Kenya's March 2026 Court of Appeal judgment, which clarified the constitutional boundaries of the Computer Misuse and Cybercrimes Act in line with Articles 33 and 34 of the Constitution, demonstrates that Kenya already has the institutional maturity to uphold this standard domestically. Malabo ratification would extend that standard to the continental level, providing Kenya with formal standing to advocate for consistent implementation across all State Parties.[105,164,165]

COUNTRY	STATUS	DATA PROTECTION	CYBERSECURITY	E-TRANSACTIONS	KEY LESSON FOR KENYA
Senegal	Ratified 2016	High: Commission de Protection des Données Personnelles (CDP) active, quarterly reports	Strong: Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI)/Centre National Opérationnel de Cybersécurité (CNOC), Penal Code integration	Strong: Law No. 2008-08; ARTP ensures secure infrastructure	Early ratification + financial autonomy = enforcement credibility
Ghana	Ratified 2019	High: 1,200+ controllers, 150+ audits/yr	Strong: Cyber Security Authority (CSA), mandatory licensing (2024)	Moderate: predates Malabo; 2025 Bill updates emerging tech	Licensing creates sustainable revenue; gender provisions fill Malabo gap
Rwanda	Ratified 2019	High: Data Protection Office (DPO), extraterritorial rules 2025	Strong: National Cyber Security Authority (NCSA), 2024–2029 Strategy	Advanced: Fintech Passporting February 2025	Integrated governance model (DPO within NCSA) enables rapid breach response; Fintech Passporting Feb 2025; AI policy leadership

Table 8

COUNTRY	STATUS	DATA PROTECTION	CYBERSECURITY	E-TRANSACTIONS	KEY LESSON FOR KENYA
Uganda	Neither signed nor ratified	Moderate: Personal Data Protection Office (PDPO) under National Information Technology Authority—Uganda (NITA-U); Google	Partial: vague 2022 amendments used against dissenters	Moderate: 2011 laws; 2025 tax digital-ID linkage	Non-ratification = no external rights anchor; enforcement gaps
Tunisia	Signed 2019; not ratified	Partial: National Authority for the Protection of Personal Data (INPDP) lacks sanctions power	Divergent: National Cybersecurity Agency (ANCS) positive; Decree-Law 54 repressive	High: Startup Act, TunTrust	Rights erosion accelerates without binding supranational commitments
Kenya	Neither signed nor ratified; Cabinet approved process step towards accession (Sept 2025)	Strong: Data Protection Act (DPA) 2019, hybrid-independence Office of the Data Protection Commissioner (ODPC)	Partial: Computer Misuse and Cybercrimes Act (CMCA) 2018 lacks Art 25(3) safeguard	Moderate: Kenya Information and Communications Act (KICA) 1998, outdated	Ratification + 'Malabo Plus' reforms = rights anchor + trade enabler

Table 8

Cybersecurity Pillar: Country Alignment with Malabo Articles 24–31

COUNTRY	National Cyber Strategy (ART 24)	CERT/CIRT Established	Core Offences Criminalised (Art 29)	Art 25(3) Human Rights Safeguard	Mutual Assistance & Cooperation (Art 28)
SENEGAL (Ratified)	Strong	Strong	Strong	Partial	Strong
GHANA (Ratified)	Strong	Strong	Strong	Partial	Strong
RWANDA (Ratified)	Strong	Strong	Strong	Partial	Strong
UGANDA (Not Signed)	Strong	Partial	Partial	Divergent	Absent
TUNISIA (Signed)	Strong	Strong	Partial	Divergent	Absent
KENYA (Cabinet approved process step towards accession 2025)	Strong	Strong	Partial	Partial	Absent

Figure 8: Cybersecurity Pillar — Country Alignment with Malabo Articles 24–31. Six countries, five indicators. Starred annotations: Kenya s.22/23 ruling (March 2026). Source: Comparative analysis, Section V; AU Convention Arts 24–31; BAKE v AG (endnotes 39, 80, 102–106, 164)

The Data Protection Pillar matrix (Figure 9) illustrates that Kenya's DPA 2019 achieves strong alignment with Malabo's Articles 9–23 on consent and data subject rights, but reveals a gap on cross-border transfer mechanisms (Article 14). The February 2026 CBK M-Pesa phone-number masking approval — implementing the DPA's data-minimisation principle — is a significant practical demonstration that Kenya's regulatory system is already operationalising Malabo standards.[7,169,170]

Data Protection Pillar: Country Alignment with Malabo Articles 9-23

COUNTRY	Independent Authority (Art 11)	Consent & Minimisation (Art 13)	Subject Rights (Arts 16-19)	Transborder Flow Rules (Art14(6))	Enforcement Capacity & Sanctions
SENEGAL (Ratified)	Strong	Strong	Strong	Strong	Strong
GHANA (Ratified)	Partial	Strong	Strong	Partial	Strong
RWANDA (Ratified)	Partial	Strong	Strong	Strong	Partial
UGANDA (Not Signed)	Divergent	Strong	Partial	Partial	Partial
TUNISIA (Signed)	Partial	Partial	Partial	Absent	Absent
KENYA (Cabinet approved process step towards accession 2025)	Partial	Strong	Strong	Partial	Partial

Figure 9: Data Protection Pillar — Country Alignment with Malabo Articles 9–23. Starred annotation: CBK M-Pesa masking approval (February 2026). Source: Comparative analysis, Section V; DPA 2019; CBK approval Feb 2026 (endnotes 7, 34–37, 102–106, 148)

The Electronic Transactions Pillar matrix (Figure 10) reveals that Kenya's consumer e-commerce protections under the Kenya Information and Communications Act Cap 411A remain the weakest link in its digital governance architecture. Ghana's Electronic Transactions Act 2008 and Rwanda's ICT Law provide the Malabo-aligned legislative templates that Kenya's forthcoming digital commerce reform programme should adopt.[38,40,69]

Electronic Transactions Pillar: Country Alignment with Malabo Articles 1-8

COUNTRY	Legal Validity of E-Contracts (Art 6)	E-Signature Recognition (Art 3)	Consumer Protection (Art 8)	Cross-Border Recognition & MoUs	Emerging Tech (AI/Fintech Blockchain)
SENEGAL (Ratified)	Strong	Strong	Strong	Partial	Partial
GHANA (Ratified)	Strong	Strong	Strong	Strong	Partial
RWANDA (Ratified)	Strong	Strong	Strong	Strong	Strong
UGANDA (Not Signed)	Strong	Partial	Partial	Absent	Absent
TUNISIA (Signed)	Strong	Strong	Strong	Absent	Partial
KENYA (Cabinet approved 2025)	Strong	Strong	Partial	Strong	Partial

Figure 10: Electronic Transactions Pillar — Country Alignment with Malabo Articles 1–8. Starred annotation: CBK–NBR Licence Passporting MoU (11 March 2026). Source: Comparative analysis, Section V; CBK–NBR MoU March 2026 (endnotes 65, 72, 73, 167, 168)

G. Multi-Year Empirical Analysis: 2013–2026

Figures 11 and 12 extend the comparative analysis beyond the 2024 snapshot by tracing all six countries across a decade of data, starting from 2013 — the year before the Malabo Convention was adopted. This multi-edition analysis demonstrates that ratification correlates with measurable, sustained improvements in cybersecurity governance and digital connectivity, not merely with paper compliance.

Internet Penetration Trends 2013-2023: Six Malabo Comparator Countries
Pre-Malabo baseline through post-ratification digital expansion (World Bank WDI)

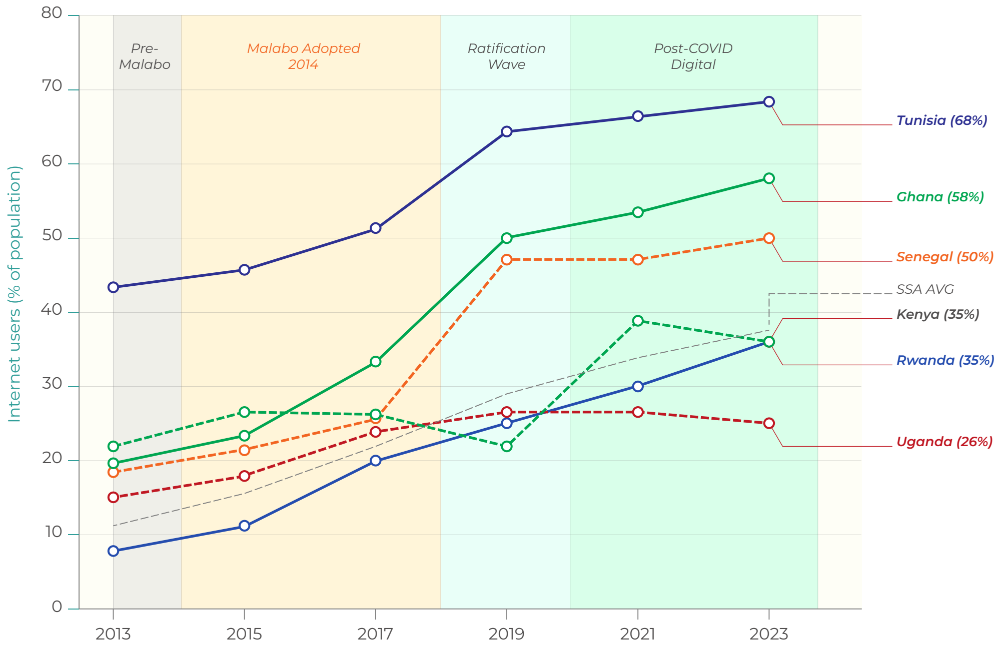


Figure 11: Internet Penetration 2013–2023 — Six Malabo Comparator Countries. Sources: World Bank WDI indicator IT.NET.USER.ZS; ITU DataHub. Kenya 2019 (22.7%): Kenya Housing Survey. Kenya 2021 (38.25%): TheGlobalEconomy.com citing World Bank. Sub-Saharan Africa average: GSMA/ITU composite. Endnotes 179, 180, 186.

Note: Series ends 2023; 2024 snapshot at Figure 7 Panel B.

This section steps back from the 2024 snapshot to trace all six comparator countries across a full decade, from 2013 — the year before the Malabo Convention was adopted — to 2026. The purpose is to test whether ratification correlates with measurable, sustained improvement in cybersecurity governance and digital connectivity, or merely with paper compliance. By following the same indicators (the ITU GCI, internet penetration, and mobile-economy value) over time rather than at a single point, the analysis isolates the longitudinal effect of the Convention's framework and provides the empirical foundation for the ratification case in Section VI.

Multi-Index Convergence Dashboard 2013–2026

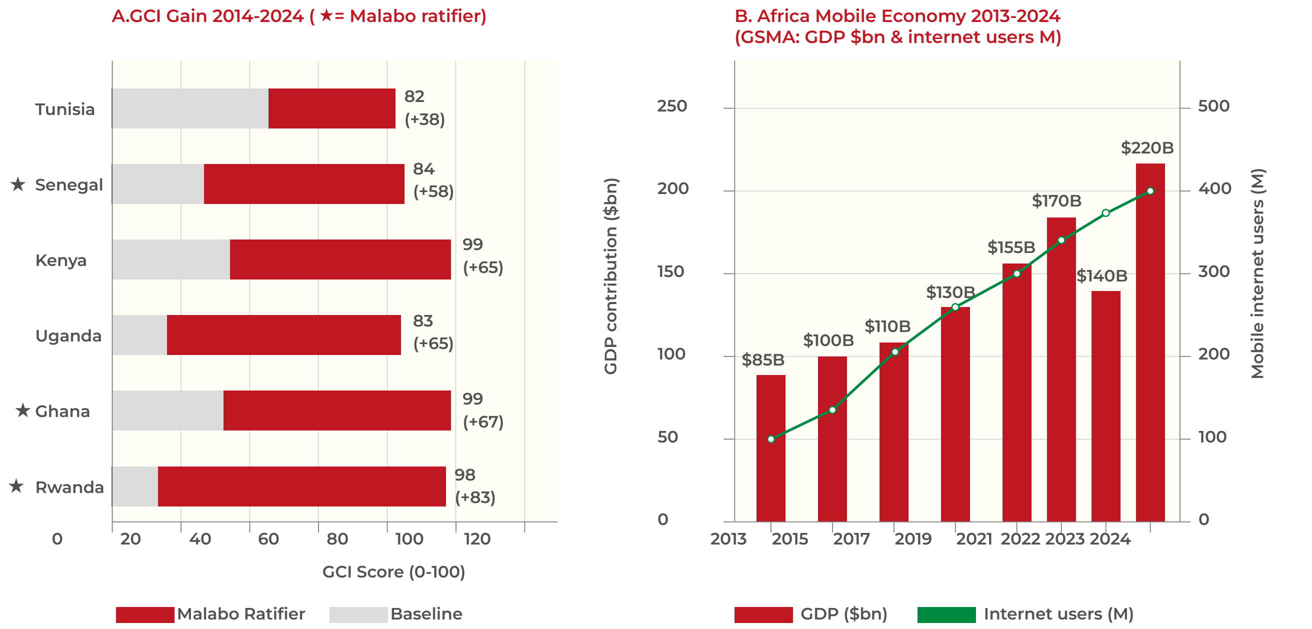


Figure 12: Multi-Index Analysis — GCI Trajectory Gains & Africa Mobile Economy. Panel A: GCI improvement 2014–2024 per country (GCI 2014 normalised ×100).★= Malabo ratifier. Panel B: Africa mobile economy GDP contribution ($bn) and mobile internet users (millions) 2013–2024 (GSMA). Sources: ITU GCI 2014–2024 (ENs 178, 184, 185); GSMA Mobile Economy Africa/SSA 2018–2025 (EN 187).

** Senegal GCI 2024 score estimated; ITU official score pending publication confirmation.*

C. Malabo Ratification Status vs. GCI Performance (all editions, normalised 0-100)

COUNTRY	MALABO STATUS	2014	2020	2024	GCI 2024 Tier
KENYA	Cabinet Approved Sep 2025	33.8	95.7	98.6	Tier 1
GHANA	Ratified May 2019	31.9	77.4	99.3	Tier 1
RWANDA	Ratified Nov 2019	15.6	73.3	98.1	Tier 1
SENEGAL	Ratified Aug 2016	26.9	64.1	84.5	Tier 2*
UGANDA	Not Ratified	17.5	40.2	82.9	Tier 3
TUNISIA	Signed, not ratified	44.4	67.8	82.0	Tier 3

Figure 12a

** Senegal GCI 2024 score estimated; ITU official score pending publication confirmation.*

This table sets each comparator's Malabo status against its GCI score across all editions (normalised 0–100). Read together, the rows show a consistent relationship: the earliest ratifiers — Ghana (2019) and Rwanda (2019) — record both the highest current scores and the largest decade-long gains, while non-ratifiers and signatories trail. Kenya, already a Tier 1 performer, has the domestic capability the Index rewards; what the table isolates is the treaty layer that the leading performers added to that capability and Kenya has not yet adopted.

D. Policy Events & Index Milestones: 2013-2026

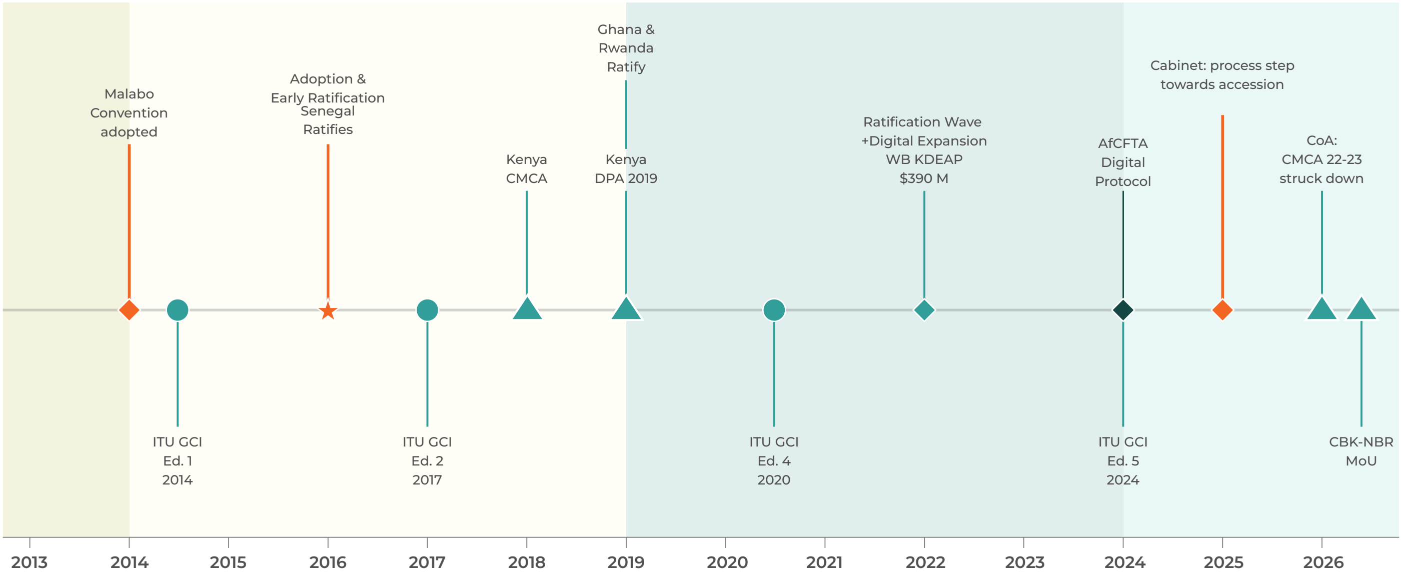


Figure 12b: Multi-Index Analysis — Ratification Status vs GCI Performance & Policy Timeline. Panel C: Malabo ratification status against GCI scores across all editions (normalised 0–100). Panel D: Policy events and index milestones 2013–2026. Sources: ITU GCI editions 2014–2024 (ENs 178, 184, 185); AU Treaty database for ratification status; policy events from EN 7, 38, 164–170, 175–183.

Panel A confirms that the two countries with the earliest and most complete Malabo ratifications — Ghana (+67 normalised points, 2019) and Rwanda (+82, 2019) — achieved the largest absolute GCI gains of any comparator over the decade, overtaking Kenya between the 2017 and 2020 editions despite starting from lower baselines. Kenya's 2014 score was already the highest in the group (33.8 normalised), reflecting its early digital infrastructure investment; the fact that Rwanda and Ghana overtook it suggests the Malabo framework provides structural acceleration beyond organic development.[178,184,185]

Panel B shows Africa's mobile economy grew from $85 billion to $220 billion between 2013 and 2024 — a 159% increase. With 416 million mobile internet users and $712 billion in projected AfCFTA digital market value by 2050, the cooperation deficit documented in Section III.E and IV.D is not static but expanding. Panel D traces the full decade: Malabo adoption (June 2014), Kenya's CMCA (2018) and DPA (2019), the ratification wave, the September 2025 Cabinet accession approval, and the March 2026 Court of Appeal ruling — all converging on the same legislative step.[180,181,183]

The aggregate finding of the multi-year analysis is unambiguous: the countries that ratified Malabo earlier built stronger, faster-improving digital governance frameworks. Kenya, already a GCI Tier 1 performer and ITU Regulatory Tracker #1 in Africa, has demonstrated all the domestic capabilities required. What remains is the treaty layer that connects those capabilities to the 20 states that have already built their cooperation frameworks around Malabo's architecture.[178,182]

- **Data protection Gaps**
  The Data Protection Act (DPA) caps fines at KES 5 million or 1% of turnover, insufficiently deterrent for global technology companies. Malabo encourages a flexible, harmonised sanctioning regime enabling Kenyan regulators to enforce compliance more effectively.
- **Cybersecurity safeguards:**
  The Computer Misuse and Cybercrimes Act (CMCA) lacks Malabo Article 25(3)'s explicit human-rights override. This 'supremacy clause' for digital rights would ensure that national-security exemptions cannot be used to justify blanket surveillance.
- **Breach notification:**
  Malabo's prompt notification requirement would address a gap in the Data Protection Act (DPA), protecting Kenyan citizens from delayed responses to data breaches.

H. Enhancing Policy Coherence and Regional Collaboration

Through its Open Government Partnership (OGP) membership, Kenya has committed in its 5th National Action Plan 2023–2027 to establishing a Data Governance Council and a comprehensive data capacity improvement programme.[41] Malabo provides the critical regional framework to realise these ambitions. Non-ratification risks Kenya's data regime being classified as 'inadequate' by other African Continental Free Trade Area (AfCFTA) trading blocs, creating non-tariff barriers for Kenyan businesses expanding onto the continent.[15]

I. Asserting African Ownership and Digital Sovereignty

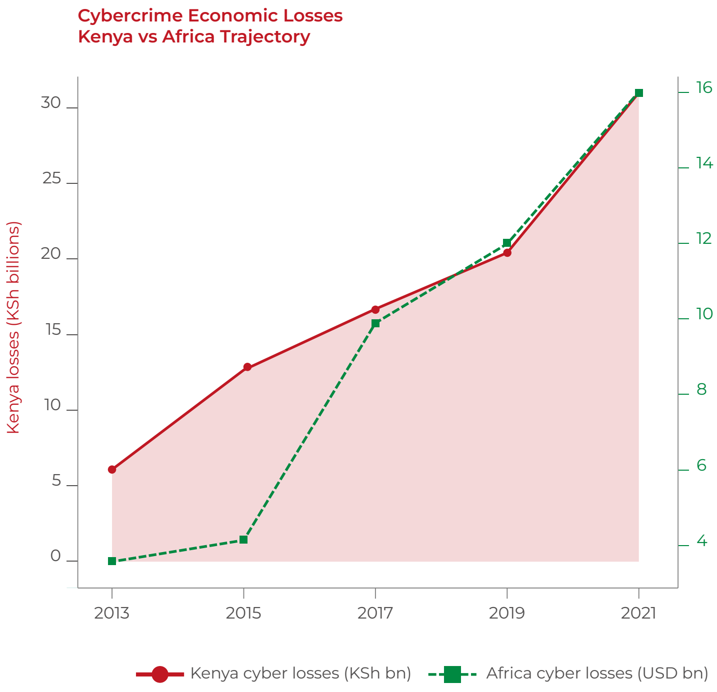
Ratification empowers Kenya to assert African ownership of digital governance, reducing reliance on external frameworks. By harmonising laws under an Africa-centric framework, Kenya can mitigate risks of 'digital colonialism' — where global technology companies extract data from African populations without local oversight. Importantly, only State Parties can propose amendments to the Convention. Ratifying would enable Kenya to advocate from within for revisions to address current weaknesses, including Artificial Intelligence (AI) governance, mandatory breach notifications, and stronger authority-independence criteria.[17]

VI Rationale for Ratification
Strengthening Kenya’s Digital Governance Architecture

Kenya's domestic framework, while comparatively strong, cannot resolve the following structural deficits in isolation.

A. Strengthening the Legal Framework for Digital Rights

Figure 13 presents the investment case in visual form: the trajectory of Kenya's cybercrime losses against the projected economic value of the AfCFTA digital market, demonstrating that the cooperation gap is not merely a legal formality but a material economic risk.



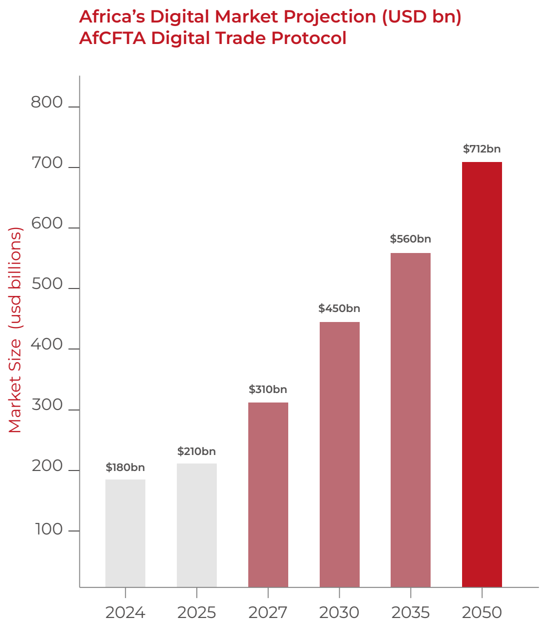


Figure 13: Cybercrime Economic Losses vs AfCFTA Digital Trade Opportunity — The Investment Case for Ratification. Sources: CA Kenya Cyber Threat Report 2025; Serianu Africa Cybersecurity 2024; AfCFTA Secretariat; ITU/IFC projections (endnotes 34, 183)

VII Barriers to Adoption and Opportunities for Reform

Thematic analysis of Key Informant Interviews (KIIs) conducted in August 2025 identifies seven recurring barriers, each paired with a corresponding opportunity.

Key informant Interview (KII) Thematic Map

KII Respondent (Role & Sector)	Perceived Sufficiency	Sovereignty & Security	Resource Constraints	Awareness Gap	Brussels Effect	Media/Press Freedom	Strategic Bloc Effect
Senior Official Office of the Data Protection Commissioner (ODPC)	✓	✓	✓	✓	—	—	✓
Regulatory Affairs Council Media Council of Kenya (MCK)	✓	—	✓	✓	—	✓	—
Human Rights Practitioner Amnesty International Kenya	✓	✓	✓	✓	—	—	—
Independent Legal Expert Advocate, High Court of Kenya (Legal Informatics)	✓	✓	✓	✓	✓	—	✓
Senior Representative Data Protection Governance Society of Kenya(DPGSK)	✓	✓	—	✓	✓	—	—
Research Consultant Law, Technology & Data Rights	✓	✓	✓	✓	—	—	—
Senior Official Communications Authority of Kenya (CA)	✓	✓	✓	✓	—	—	—
Senior Advocacy Official Bloggers Association of Kenya (BAKE)	—	✓	✓	✓	—	—	—

Figure 14: Key Informant Interview (KII) Thematic Map — Seven Recurring Themes from August 2025 KII Research

1. Perceived Sufficiency of Domestic Frameworks

A prominent theme is the belief that Kenya's existing laws are more modern or robust than the Malabo Convention. A representative of the Data Protection Governance Society of Kenya (DPGSK) stated: 'Data Protection Act (DPA) is quite progressive in terms of independence (though limited) and implementation ... It could therefore be said to be higher than Malabo.'[118] A research consultant in law, technology and digital rights observed that the Data Protection Act (DPA) has 'a more robust enforcement mechanism', reinforcing the perception of redundancy.[119] A senior official from the Office of the Data Protection Commissioner (ODPC) highlighted operational gaps, noting that 'penalties are not prohibitive' and that 'statutory time limitations ... hinder conducting thorough investigations ... especially when investigating big tech companies.'[8]

On the procedural dimension, a senior official from the Office of the Data Protection Commissioner (ODPC) confirms that the Attorney General (AG) has formally cleared the Convention for ratification, but the process has stalled twice due to successive cabinet reshuffles interrupting the approval cycle — a bureaucratic, not principled, obstacle that advocates should name plainly and address through direct engagement with the Cabinet Secretariat.[8] The same source further notes that the original 'lumping' of security with data protection 'killed' civil society momentum, diverting Civil Society Organisation (CSO) attention to the African Court as an alternative mechanism; however, a new window now exists to remobilise this constituency in support of rights-respecting ratification.[118]

- **Opportunity**
  Advocates should reframe Malabo as the 'missing link' — highlighting specific gaps such as the absence of Artificial Intelligence (AI) regulation, the lack of cross-border enforcement mechanisms, and the absence of Article 25(3)'s rights safeguard. Ratification also grants Kenya a seat at the table to propose Convention amendments addressing these weaknesses.

2. Sovereignty and National Security Concerns

A digital rights advocate from the Bloggers Association of Kenya (BAKE) noted a 'preference among the political class in Kenya to establish domestic laws that address cybersecurity, rather than adopting a continental convention.'[105] A human rights practitioner from Amnesty International Kenya emphasised that the 'lumping of security issues with data protection 'killed' the momentum and support within civil society.'[103] A senior official from the Communications Authority of Kenya (CA) cited 'political, legal, or economic factors' including resource implications and the view that 'ratification comes with obligations.'[120]

- **Opportunity**
  Kenya can utilise the Interpretative Declaration mechanism. The government can ratify the Convention with a specific declaration clarifying that the Convention's Article 1 definitions and matters of national-security data remain under exclusive sovereign control, while fully committing to the human-rights safeguards in Article 25(3) and the safeguards clause at Article 33. Only State Parties can propose amendments — ratification grants Kenya a legitimate voice to address the Convention's shortcomings from within.

3. Resource Constraints

An independent legal expert described ratification delays as resulting from 'a complex interplay of legal realities, strategic policy choices, and competing stakeholder interests', including resource implications for capacity building.[104] A senior official from the Communications Authority of Kenya (CA) specifically called for a costed implementation roadmap and a high-level political champion to steer the ratification treaty through the parliamentary process.[120]

- **Opportunity**
  Kenya can adopt the 'Ghana Model' of financing. Ratification does not require creating new bodies — it requires empowering existing ones (Office of the Data Protection Commissioner (ODPC) and National Computer and Cybercrimes Co-ordination Committee (NC4)). Advocates should demonstrate how ratification enables these bodies to generate revenue through harmonised regional licensing schemes, ensuring financial sustainability while maintaining fiscal sustainability.

4. Awareness Gaps

A human rights practitioner from Amnesty International Kenya observed that 'awareness of the Malabo Convention among stakeholders in Kenya is generally low, especially outside of the core group of digital rights activists and legal experts.'[103] A digital rights advocate from the Bloggers Association of Kenya (BAKE) echoed this, noting gaps due to technical complexity and lack of public education.[105] Independent analysis notes that emerging awareness exists in the business community as cross-border e-commerce takes root, with key interest in harmonised data flows and legal compliance.[104]

- **Opportunity**
  A 'Demystification Campaign' translating the Convention's complex provisions into relatable narratives — such as safer mobile-money transactions for Small and Medium-Sized Enterprises (SMEs) and stronger privacy rights for citizens — can generate the bottom-up pressure needed to break political inertia. A research consultant in the field specifically recommends accessible formats including infographics, short explainer videos, and bilingual (English/Swahili) summaries.

5. The Media and Press Freedom Dimension

A discrete and underappreciated barrier concerns the specific vulnerabilities of the media and journalism sector. A regulatory affairs official from the Media Council of Kenya (MCK) highlighted that journalists face unique exposure under the Computer Misuse and Cybercrimes Act (CMCA)'s false-publication provisions, which carry risks of prosecution that chill legitimate investigative reporting.[117] The Media Council of Kenya (MCK) is actively collaborating with the Office of the Data Protection Commissioner (ODPC) to develop journalist-specific data protection guidelines — a concrete initiative demonstrating practical demand for a clearer legal framework. Regional media houses operating across borders face particular uncertainty, as differing data-protection regimes across African jurisdictions create compliance burdens that harmonisation under the Malabo Convention would help resolve.

- **Opportunity**
  The Media Council of Kenya (MCK)–Office of the Data Protection Commissioner (ODPC) collaboration on journalist guidelines should be explicitly referenced in Kenya's ratification instrument as a commitment to implementing the Article 25(3) safeguards in a sector-specific manner.

6. The Brussels Effect: Competing Regulatory Frameworks

A structural barrier identified by a representative of the Data Protection Governance Society of Kenya (DPGSK) has identified 'Brussels Effect': the tendency of states with strong domestic frameworks to adopt General Data Protection Regulation (GDPR)-aligned legislation as a route to European Union (EU) data adequacy decisions, potentially viewing Malabo as redundant or in tension with their European Union (EU)-oriented regulatory strategy.[118] Kenya's Data Protection Act (DPA) 2019 was consciously modelled on the General Data Protection Regulation (GDPR), and there is an argument within policy circles that prioritising General Data Protection Regulation (GDPR) alignment is more commercially advantageous than Malabo ratification. This framing presents a false dilemma: the Malabo Convention and General Data Protection Regulation (GDPR) alignment are not mutually exclusive. Ghana holds both the Malabo and Budapest Convention ratifications and is actively pursuing European Union (EU) data-adequacy discussions. Moreover, the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol — which will govern Kenya's largest continental market — is anchored in Malabo-compatible frameworks, not General Data Protection Regulation (GDPR) structures.

- **Opportunity**
  Kenya can pursue General Data Protection Regulation (GDPR) adequacy and Malabo ratification together rather than treating them as alternatives. Ghana already holds both the Malabo and Budapest Convention ratifications while actively pursuing European Union (EU) data-adequacy discussions, showing the two tracks are complementary. Because the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol — which

governs Kenya’s largest continental market — is anchored in Malabo-compatible frameworks rather than GDPR structures, ratification positions Kenya to access both the European and the continental markets at once. The ‘Brussels Effect’ is therefore not a reason to defer Malabo but a parallel commercial pathway that ratification complements.

7. The Strategic Bloc Effect and Anticipated Reservations

A senior legal informatics expert identified a structural pattern: Kenya belongs to a cohort of Africa's most digitally advanced economies — alongside Nigeria, South Africa, Ethiopia, Morocco, and Egypt — that have collectively withheld Malabo ratification. Ghana is a notable exception. Non-ratification is not bureaucratic delay; it represents a deliberate strategic choice by states with the most significant regulatory autonomy interests to protect.[104]

Compounding this are specific legal concerns: the Office of the Data Protection Commissioner (ODPC) has indicated Kenya may seek to enter interpretative declarations or reservations on certain Convention provisions. The provisions in question include the scope clauses at Article 9 (defining what falls within and outside the personal-data-protection regime, including the household-processing exemption at Article 9(2)(a)) and the sensitive-data regime at Article 14 (which prohibits processing of sensitive personal data subject to the exceptions enumerated at Article 14(2)).[85] The Convention does not contain a dedicated reservations clause; reservations or interpretative declarations would be deposited under the customary international law of treaties (Vienna Convention on the Law of Treaties, Article 19) and noted at the time of deposit of the instrument of ratification under Article 35. However, reservations on Article 14 (the sensitive-data prohibition and its exceptions) could weaken protections for sensitive personal data — including health and ethnicity data — categories of particular relevance given Kenya's ethnic diversity and its experience of data-related election harms.

- **Opportunity**
  Civil society must engage proactively on the specific reservation articles. Rather than opposing reservations wholesale, Civil Society Organisations (CSOs) should conduct a human-rights impact assessment of each proposed reservation, provide evidence-based submissions to the Attorney General's Office, and propose narrowly tailored interpretative declarations that address government concerns without creating substantive rights gaps. This is the difference between advocating for 'Malabo Plus' and conceding to 'Malabo Minus'.

VIII Policy Recommendations

A. For the Government of Kenya (Executive and Parliament)

1. Expedite ratification with strategic declarations

The Cabinet should approve ratification of the Malabo Convention promptly, building on the Office of the Data Protection Commissioner (ODPC)'s September 2025 stakeholder consultations. The ratification instrument should include an interpretative declaration affirming Kenya's sovereignty over national-security data while fully committing to the human-rights safeguards in Article 25(3) and the safeguards clause at Article 33. Parliament should prioritise debates in the Information and Communication Technology (ICT) Committee and ensure the process complies with Article 118 of the Constitution on public participation.

2. Conduct a formal 'Legislative Gap Analysis'

The Attorney General's Office should map Malabo against the Data Protection Act (DPA) 2019 and Computer Misuse and Cybercrimes Act (CMCA) 2018 to identify specific amendments required rather than a wholesale overhaul. This audit should be led by a multi-stakeholder task force including legal experts, civil society representatives, and independent academics, and should be completed within six months of ratification.

3. Enact a 'Malabo Implementation Act'

Rather than amending laws piecemeal, Parliament should consider an omnibus bill that: (a) updates the Computer Misuse and Cybercrimes Act (CMCA) by explicitly incorporating the Article 25(3) human-rights override and amending sections 22, 23, and 27; (b) amends the Data Protection Act (DPA) 2019 to introduce higher, dissuasive penalties aligned with regional standards; and (c) updates the Kenya Information and Communications Act (KICA) with modern electronic-transactions provisions covering blockchain and Artificial Intelligence (AI).

4. Launch a 'Kenyan New Deal' for Digital Governance

The Ministry of Information, Communications and the Digital Economy should develop a strategy mirroring Senegal's New Deal Technologique (NDT), explicitly linking ratification to the Digital Master Plan 2022–2032. This strategy should secure dedicated budget for Office of the Data Protection Commissioner (ODPC) and National Computer and Cybercrimes Co-ordination Committee (NC4) operationalisation.

5. Develop a 'Data Protection Fund'

Amend the Data Protection Regulations to permit the Office of the Data Protection Commissioner (ODPC) to retain a defined percentage of administrative fines and controller registration fees, reducing dependence on exchequer funding and enhancing enforcement capacity — modelled on Ghana's Cyber Security Authority (CSA) approach.

6. Conduct human-rights impact assessments on proposed reservations

Before finalising any reservations or interpretative declarations, the Attorney General's Office should publish a human-rights impact assessment and invite civil society submissions.

B. For the Private Sector

7. Frame ratification as a cost-reduction mechanism

Businesses should understand that Malabo ratification reduces compliance fragmentation across borders, enabling Kenyan companies — including fintechs such as M-Pesa — to expand regionally under the African Continental Free Trade Area (AfCFTA) with a harmonised, predictable regulatory framework.

8. Participate in public–private cybersecurity partnerships

Following Ghana's model, the private sector should actively partner with the Communications Authority of Kenya (CA)/National Computer and Cybercrimes Co-ordination Committee (NC4) to co-fund national cybersecurity awareness and licensing programmes, contributing to a self-sustaining financing model.

C. For Civil Society, Human Rights Defenders, and Academia

9. Shift from opposition to constructive advocacy

Civil society should move beyond general opposition to the Convention and engage constructively by proposing specific legal safeguards — for marginalised groups including women, youth, and persons with disabilities — to be attached to the ratification instrument.

10. Establish a 'Digital Rights Observatory'

A coalition of Civil Society Organisations (CSOs) should monitor Convention implementation post-ratification, tracking Office of the Data Protection Commissioner (ODPC) independence and Computer Misuse and Cybercrimes Act (CMCA) application, using Malabo standards as a benchmark for strategic litigation — including supporting the ongoing Bloggers Association of Kenya (BAKE) appeal against the High Court's dismissal of the Computer Misuse and Cybercrimes Act (CMCA) petition — against overreach.

11. Produce evidence on the gender gap

Academia should generate empirical data on Online Gender-Based Violence (OGBV) and the intersectional vulnerabilities of women, persons with disabilities, and rural communities in Kenya's digital landscape, supporting the drafting of a specific gender protocol to the Computer Misuse and Cybercrimes Act (CMCA).

12. Engage proactively on the proposed reservations and interpretative declarations

Civil Society Organisations (CSOs) should conduct a human-rights impact assessment of any reservations or interpretative declarations identified by the Attorney General's Office (with particular attention to the scope clauses at Article 9 and the sensitive-data regime at Article 14) and provide evidence-based submissions before ratification is finalised.

13. Leverage existing regional forums

Platforms such as the Africa Internet Governance Forum and the Forum on Internet Freedom in Africa provide existing venues for civil society to advance Malabo implementation discussions.

D. For the African Union and Regional Bodies

14. Urgently institutionalise the Article 32 implementation follow-up mechanism

The Convention's monitoring function — vested in the Chairperson of the AU Commission to report on State Party implementation to the Conference of Heads of State and Government — has not been operationally institutionalised despite the Convention's entry into force in 2023. The African Union should establish a permanent Convention Secretariat to support that function, with explicit human-rights, AI, and biometrics expertise, and should commit to regular public implementation reports.

15. Facilitate 'Best Practice' Forums

The African Union (AU) should host regional forums — including through existing mechanisms such as the Africa Internet Governance Forum — where member states share successful implementation models, such as the Rwanda–Ghana fintech passporting agreement.

16. Provide technical assistance for gap-filling revisions

The African Union (AU) should engage member states in updating the Convention to address the absence of mandatory breach-notification timelines, Artificial Intelligence (AI) governance provisions, and detailed authority-independence criteria.

IX Conclusion: A Call to Action for a Secure Digital Future

Kenya stands at a decisive moment in its digital governance journey. The evidence assembled in this Brief — drawn from ITU data, World Bank indicators, GSMA research, comparative legal analysis across five African states, and the testimony of senior Kenyan practitioners — points in one direction: ratification of the Malabo Convention is not merely a diplomatic formality. It is the institutional architecture that Kenya's world-class digital economy both deserves and urgently needs.

Kenya's Digital Credentials Demand a Continental Commitment

Kenya is ranked #1 in Africa and #20 globally on the ITU ICT Regulatory Tracker 2024 and scores 98.59 on the ITU Global Cybersecurity Index 2024, placing it in the Tier 1 'role-modelling' tier alongside Ghana (99.27) and Rwanda (98.08) — two Malabo ratifiers. The World Bank's US$390 million Kenya Digital Economy Acceleration Project (KDEAP), effective February 2024, reflects the international community's confidence in Kenya's digital governance trajectory.[178,179,182]

Yet Kenya's Mutual Legal Assistance Act 2011 covers none of the 20 Malabo ratifiers. Cap 43 covers only eight countries worldwide and only civil judgments. The Computer Misuse and Cybercrimes Act 2018/2025 creates a 24/7 contact point that is best-endeavours without a binding treaty. This gap between Kenya's domestic digital leadership and its international cooperation architecture is the central vulnerability that this Brief has documented.[7,175,176,177]

Three Convergent Signals in 2025–2026

Three developments in the months preceding this Brief's publication have collectively transformed the ratification debate from an aspirational policy question into an urgent governance necessity.

Cabinet Approval (September 2025):

In September 2025, Kenya's Cabinet approved a process step towards accession to the Malabo Convention, formally clearing the executive branch barrier that had delayed action for a decade. The institutional momentum is in place; Parliament's ratification decision is the single remaining step needed to give that decision the force of binding law.

Court of Appeal ruling (6 March 2026):

On 6 March 2026, the Court of Appeal struck down sections 22 and 23 of the Computer Misuse and Cybercrimes Act as unconstitutional, vindicating the central human rights argument that underpins Malabo Article 25(3). Kenya's judiciary has affirmed the very constitutional standard that the Convention requires: cybersecurity measures must protect, not restrict, freedom of expression. Malabo ratification extends that standard continentally.[164,165]

Bilateral digital trade architecture (2025–2026):

On 11 March 2026, the Central Bank of Kenya and the National Bank of Rwanda signed a Licence Passporting Framework MoU for payment service providers — the latest in a pattern of Kenya–Rwanda bilateral digital trade architecture that demonstrates Kenya's regulatory maturity and its readiness for the continental framework that Malabo formalises.[167,168,169]

The Path Forward

The seven policy recommendations in Section VIII provide a sequenced roadmap. The immediate priority is parliamentary action: scheduling a dedicated debate on the ratification instrument, requesting a joint technical briefing from the Attorney-General, the ODPC Commissioner, and the Communications Authority, and commissioning the formal Legislative Gap Analysis that will map the DPA 2019, CMCA 2018/2025, MLA Act 2011, Cap 43, and KICA Cap 411A against Malabo's three pillars.

The medium-term legislative programme — reviewing CMCA sections 27 (parts of which remain suspended under High Court conservatory orders of 22 October 2025) and 48–53 in light of the March 2026 Court of Appeal ruling, strengthening DPA enforcement capacity for global data controllers, and modernising KICA Cap 411A to address AI, blockchain, and mandatory breach notification — is work that needs to begin regardless of ratification. Ratification provides the continental anchor that makes that work coherent and legible to Kenya's trading partners.[7,38,40]

Kenya's civil society, technical community, and legal practitioners have demonstrated through this research that they are ready to engage constructively with the ratification process. The March 2026 Court of Appeal outcome, secured through the collective advocacy of BAKE, ARTICLE 19 Eastern Africa, and the Law Society of Kenya, shows that Kenya's institutions are capable of the collaborative governance that Malabo demands.

Kenya does not need to create new institutions, sacrifice sovereignty, or await a more convenient moment. It needs to ratify. The Malabo Convention, accompanied by an Interpretative Declaration deposited at ratification under Article 35 affirming Kenya's sovereignty over national-security data, is the instrument that closes the gap between Kenya's world-class domestic digital governẨance and its continental cooperation architecture. Parliament's decision will determine whether Kenya leads Africa's digital future or watches that future be shaped by the 20 states that have already acted.

The Silicon Savannah's next chapter is a continental one. The ratification of the Malabo Convention is Kenya's entry into that chapter.

Endnotes

1. E.B. Ndemo, 'Political Entrepreneurialism: Reflections of a Civil Servant on the Role of Political Institutions in Technology Innovation and Diffusion in Kenya', Stability: International Journal of Security and Development, 4(1), 2015.
2. M. Jönsson, Political Economics of Gender Relations in Information and Communication Technologies in Agricultural Development: The Case of Knowledge-Based Platforms for Farmers in Kenya (HAL, 2018).
3. F. Soulé, 'Navigating the Multiplexity of Africa's Digital Partnerships amidst Global Rivalry', Global Studies Quarterly, 5(4), 2025.
4. J.O. Asaka and A.A. Oluoko-Odingo, 'Introduction', in Routledge eBooks, 2022.
5. K.E. Aynaoui, L. Jaïdi and A. Zaoui, Digitalise to Industrialise (Routledge eBooks, 2022). doi:10.4324/9781003274322-7.
6. M. Jönsson, ibid.
7. Republic of Kenya, Data Protection Act (Act No. 24 of 2019) (Nairobi: Government Printer, 2019); Republic of Kenya, Computer Misuse and Cybercrimes Act (Act No. 5 of 2018) (Nairobi: Government Printer, 2018).
8. Key Informant Interview, Senior Official, Complaints, Investigations and Enforcement, Office of the Data Protection Commissioner (ODPC), Nairobi, August 2025 (on file with authors).
9. M. Maseko, 'Understanding Digital Rights in an Era of Digital Politics in Africa', Digital Policy Studies, 3(1), 2024, p. 58.
10. Key Informant Interview, Senior Official, Regulatory Affairs Division, Communications Authority of Kenya (CA), Nairobi, August 2025 (on file with authors).
11. M.A. Bouke et al., 'African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions', arXiv, 2023. doi:10.48550/arxiv.2307.01966
12. T.H. Sime, 'A Critical Reflection on African Maritime Cybersecurity Frameworks', Scientia Militaria: South African Journal of Military Studies, 51(3), 2023.
13. World Trade Organization (WTO), Annual Report 2024 (Geneva: WTO, 2024).
14. J.C.S. Gummadi, 'Cybersecurity in International Trade Agreements: A New Paradigm for Economic Diplomacy', American Journal of Trade and Policy, 11(1), 2024, p. 39.
15. F. Sucker and A. Beyleveld, 'African Rules on Cross-Border Data Flows: The Significance of Regulatory Convergence and the AfCFTA Digital Trade Protocol's Potential Contribution', SSRN Electronic Journal, 2024. doi:10.2139/ssrn.4741632; African Union (AU), Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade (Addis Ababa: AU, 2024).
16. N. Mishra and K. Kugler, 'International Community in the Global Digital Economy: A Case Study on the African Digital Trade Framework', International and Comparative Law Quarterly, 73(4), 2024, p. 853.
17. Oxfam, ReCIPE Project Framework Document (Nairobi: Oxfam, 2024). https://www.oxfamrecipe.eu/
18. KICTANet, Public Participation in ICT Policy Making (Nairobi: KICTANet, 2023).
19. African Union (AU), African Union Convention on Cyber Security and Personal Data Protection (Addis Ababa: AU, 2014). https://au.int/sites/default/files/treaties/29560-treaty-0048_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
20. African Union (AU), Status List: African Union Convention on Cyber Security and Personal Data Protection (Addis Ababa: AU, as at 8 July 2024). Accessed 11 September 2025. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
21. Center for Strategic and International Studies (CSIS), Digital Africa: Leveling Up through Governance and Trade (Washington DC: CSIS, 2021).
22. African Researchers Magazine, 'The Malabo Convention: Africa's Cybersecurity and Data Protection Framework Explained', African Researchers Magazine, 24 February 2025. Accessed 20 November 2025.
23. Centre for International Governance Innovation (CIGI), Digital Sovereignty in Africa (Waterloo: CIGI, 2023).
24. B.M. Farmer, 'How Kenya Became the 'Silicon Savannah'', CBS News, 29 June 2025. Accessed 26 January 2026. https://www.cbsnews.com/news/how-kenya-became-the-silicon-savannah-60-minutes/
25. Ministry of ICT, Innovation and Youth Affairs, Kenya National Digital Master Plan 2022–2032 (Nairobi: Republic of Kenya, 2022).
26. Republic of Kenya, Kenya Vision 2030: The Popular Version (Nairobi: Government Printer, 2008).

Endnotes

27. U.S. International Trade Administration, 'Kenya — Digital Economy', Country Commercial Guide, 2024. Accessed 20 November 2025. https://www.trade.gov
28. Kenya National Bureau of Statistics (KNBS), Economic Survey 2025 (Nairobi: KNBS, 2025).
29. Central Bank of Kenya (CBK), Financial Inclusion Report 2024 (Nairobi: CBK, 2024).
30. International Telecommunication Union (ITU), Digital Development Dashboard: Africa (Geneva: ITU, 2025).
31. GSMA, The Mobile Economy Africa 2025 (London: GSMA, 2025).
32. Cybersecurity Ventures, Cybercrime Magazine Annual Report 2025 (Sausalito: Cybersecurity Ventures, 2025).
33. INTERPOL, Africa Cyberthreat Assessment Report 2025 (Lyon: INTERPOL, 2025); Serianu, Africa Cybersecurity Report — Kenya 2025 (Nairobi: Serianu, 2025); Communications Authority of Kenya (CA), Cyber Security Report Q1 2025/2026 (Nairobi: CA, 2025).
34. ODPC, Kenya Undertakes Stakeholder Consultations on Accession to the Malabo Convention (Nairobi: ODPC, 8 September 2025). https://www.odpc.go.ke
35. ODPC, Sector Specific Guidelines (Nairobi: ODPC, November 2025).
36. Human Rights Watch (HRW), Kenya: New Cybercrime Amendments (November 2025). https://www.hrw.org
37. Amnesty International Kenya, 5 Years On: DPA Perspectives (Nairobi: Amnesty International, October 2025).
38. Republic of Kenya, Computer Misuse and Cybercrimes (Amendment) Act (Act No. 17 of 2025) (Nairobi: Government Printer, 2025).
39. Bloggers Association of Kenya (BAKE) v Attorney General [2018] KEHC 9469 (KLR), 29 May 2018 (Mwita J., conservatory orders); Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020] KEHC 7924 (KLR) (substantive dismissal); reversed in part by Bloggers Association of Kenya (BAKE) v Attorney General & 6 others (Civil Appeal 197 of 2020) [2026] KECA 430 (KLR), 6 March 2026.
40. Communications Authority of Kenya (CA), KE-CIRT/CC Reports (Nairobi: CA, 2025).
41. Republic of Kenya, Open Government Partnership (OGP) 5th National Action Plan 2023–2027 (Nairobi: Republic of Kenya, 2023).
42. Access Now, Room for Improvement: A Review of the African Union Convention on Cyber Security and Personal Data Protection (Washington DC: Access Now, 2016). https://www.accessnow.org
43. N.N. Ifeanyi-Ajufo, 'Cyber Governance in Africa: At the Crossroads of Politics, Sovereignty and Cooperation', Policy Design and Practice, 6(2), 2023, p. 146.
44. K.M. Ball, 'African Union Convention on Cyber Security and Personal Data Protection', International Legal Materials, 56(1), 2017, p. 164.
45. J. Walubengo and M. Mutemi, 'Treatment of Kenya's Internet Intermediaries under the Computer Misuse and Cybercrimes Act, 2018', The African Journal of Information and Communication (AJIC), 21, 2018.
46. R. Kakungulu-Mayambala and S. Rukundo, 'Digital Activism and Free Expression in Uganda', African Human Rights Law Journal, 19(1), 2019.
47. United Nations Conference on Trade and Development (UNCTAD), Data Protection Legislation Worldwide (Geneva: UNCTAD, 2024).
48. Commission de Protection des Données Personnelles (CDP), Annual Report 2024 (Dakar: CDP, 2024). https://www.cdp.sn
49. Paradigm Initiative, The Malabo Roadmap: Advancing Data Protection and Cybercrime Frameworks in Africa (Data Protection Africa, September 2022). https://dataprotection.africa
50. Chatham House, 'The AU Can Help African Countries Adopt the UN Cybercrime Convention', 31 October 2025. Accessed 20 November 2025. https://www.chathamhouse.org
51. Presidency of the Republic of Senegal, New Deal Technologique: A National Ambition to Make Senegal a Leader in the Digital Economy in Africa (Dakar, 24 February 2025). Accessed 20 November 2025. https://www.presidence.sn
52. Presidency of the Republic of Senegal, Senegal Signs a $10 Million Strategic Partnership with the Gates Foundation (Dakar, September 2025). https://www.presidence.sn
53. Republic of Senegal, Law No. 2008-12 of 25 January 2008 on the Protection of Personal Data (Dakar: Government Printer, 2008).
54. Commission de Protection des Données Personnelles (CDP), Avis Trimestriels (Dakar: CDP, 2025). Accessed 20 November 2025. https://www.cdp.sn

Endnotes

55. Republic of Senegal, Law No. 2016-29 of 8 November 2016 (amending the Senegalese Penal Code to incorporate Arts 25 and 29 of the Malabo Convention) (Dakar: Government Printer, 2016).
56. Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI), Missions (2025). Accessed 20 November 2025. https://stcc-ssi.sn/mission/
57. Regulatory Authority for Telecommunications and Posts (ARTP), Missions et Attributions (2025). Accessed 20 November 2025. https://www.artp.sn; Republic of Senegal, Law No. 2008-08 of 25 January 2008 on Electronic Transactions (Dakar: Government Printer, 2008).
58. IC Africa, 'Ghana's 1Q2025 Real GDP Growth Update', June 2025. Accessed 20 November 2025. https://ic.africa
59. Republic of Ghana, Data Protection Act, 2012 (Act 843) (Accra: Government Printer, 2012).
60. Data Protection Commission (DPC), Annual Report 2024 (Accra: DPC, 2024). https://moc.gov.gh/dpc/
61. Republic of Ghana, Cybersecurity Act, 2020 (Act 1038) (Accra: Government Printer, 2020).
62. Cyber Security Authority (CSA), Press Release: Licensing and Accreditation Post-Deadline Enforcement (Accra: CSA, 11 January 2024); e-Crime Bureau, '51 Cybersecurity Service Providers Certified by CSA', Accra, 11 July 2024.
63. Republic of Ghana, Cybersecurity (Amendment) Bill 2025 (Accra: Government Printer, 2025).
64. GhanaFact, 'Draft 2025 Cybersecurity Bill: CSA's New Functions and Police Powers', 11 November 2025. Accessed 20 November 2025. https://ghanafact.com
65. Republic of Ghana, Electronic Transactions Act, 2008 (Act 772) (Accra: Government Printer, 2008).
66. National Institute of Statistics of Rwanda (NISR), GDP National Accounts (First Quarter 2025) (Kigali: NISR, 20 June 2025). Accessed 20 November 2025. https://www.statistics.gov.rw
67. Republic of Rwanda, Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy (Kigali: Government Printer, 2021).
68. Data Protection Office (DPO), Annual Report 2024 (Kigali: DPO, 2024). https://dpo.gov.rw
69. Digital Cooperation Organization (DCO), Rwanda: Digital Economy Report (Riyadh: DCO, 2025). https://dco.org
70. Data Protection Office (DPO), Guidance on Data Protection Officer Designation (Kigali: DPO, 2024). Accessed 20 November 2025. https://dpo.gov.rw
71. Ministry of ICT and Innovation (MINICT), National Cybersecurity Strategy of the Republic of Rwanda 2024–2029 (Kigali: MINICT, 2024).
72. Global Finance and Technology Network (GFTN), 'Ghana and Rwanda to Implement Africa's First Fintech License Passport Framework', 3 March 2025. Accessed 20 November 2025. https://gftn.co
73. C. Onyango, 'Fintech Passport: Why a Ghana License Now Works in Rwanda and Vice Versa', Finance in Africa, 5 November 2025. Accessed 20 November 2025. https://financeinafrica.com
74. Republic of Rwanda, Law No. 60/2018 of 13 August 2018 on Prevention and Punishment of Cyber Crimes (Kigali: Government Printer, 2018).
75. Uganda Bureau of Statistics (UBOS), Annual Gross Domestic Product: Fiscal Year 2024/25 (Kampala: UBOS, October 2025). Accessed 20 November 2025. https://www.ubos.org
76. World Intellectual Property Organization (WIPO), Global Innovation Index 2025: Uganda Profile (Geneva: WIPO, 2025). Accessed 20 November 2025. https://www.wipo.int
77. N. Muhairwe, Analysing the Challenges in Enforcement of Data Protection Laws in Uganda (Master's thesis, Uganda Christian University, 2024). https://scholar.ucu.ac.ug
78. Uganda Registration Services Bureau (URSB), Uganda's Data Protection Office Finds Google in Breach of Privacy (Kampala: URSB, 12 August 2025). Accessed 20 November 2025. https://ursb.go.ug
79. Ministry of ICT and National Guidance, National Cybersecurity Strategy 2022–2026 (Kampala: MoICT, 2022).
80. Human Rights Watch (HRW), Uganda: Computer Misuse Act Used to Suppress Dissent (2023). Accessed 20 November 2025. https://www.hrw.org
81. Human Rights Watch (HRW), World Report 2024: Uganda (2024). https://www.hrw.org
82. KPMG, Uganda Tax (Amendment) Bills 2025 — Analysis (April 2025). Accessed 20 November 2025. https://kpmg.com
83. Oxfam in ReCIPE and Al Khatt, Policy Paper on the Legal Framework on Cybercrime in Tunisia (20 January 2026). https://www.oxfamrecipe.eu/
84. Republic of Tunisia, Organic Law No. 2004-63 of 27 July 2004 on the Protection of Personal Data (Tunis: Government Printer, 2004).

Endnotes

85. Access Now, Tunisia: Data Protection Law Reform Must Prioritize Human Rights (2024). Accessed 20 November 2025. https://www.accessnow.org
86. Republic of Tunisia, Decree-Law No. 2023-17 of 11 March 2023 on Cybersecurity (Tunis: Government Printer, 2023).
87. Committee to Protect Journalists (CPJ), 'The Law Powering Tunisia's Crackdown on the Press', 19 December 2025. Accessed 26 January 2026. https://cpj.org
88. Amnesty International, Tunisia 2024: The State of the World's Human Rights (29 April 2025). Accessed 20 November 2025. https://www.amnesty.org
89. Startup Genome, Tunisia — Ecosystem (2025). Accessed 20 November 2025. https://startupgenome.com
90. Internet Society, Personal Data Protection Guidelines for Africa (Reston: Internet Society, 2018). https://www.internetsociety.org
91. ODPC, Strategic Plan 2023–2027 (Nairobi: ODPC, 2024).
92. Republic of Rwanda, 4th Industrial Revolution Strategy 2020–2025 (Kigali: Government Printer, 2020).
93. World Bank, Digital Economy for Africa (Washington DC: World Bank, 2024).
94. African Union (AU), Malabo Roadmap (Addis Ababa: AU, 2022).
95. CIPESA, Privacy and Data Protection in the Digital Era (Kampala: CIPESA, n.d.). https://cipesa.org
96. Carnegie Endowment for International Peace, 'Continental Cyber Security Policymaking: Implications of the Entry into Force of the Malabo Convention for Digital Financial Systems in Africa', 10 July 2023. Accessed 20 November 2025. https://carnegieendowment.org
97. B. Yusuf, Robust Digital Governance Frameworks in Africa (Waterloo: CIGI, 2023).
98. Chatham House, 'The AU Took Important Action on Cybersecurity at Its 2024 Summit', 23 February 2024. Accessed 20 November 2025. https://www.chathamhouse.org
99. Future of Privacy Forum (FPF), RECs: Towards a Continental Approach to Data Protection in Africa (Washington DC: FPF, February 2024). https://fpf.org
100. Develop Local, Digital Data Rights Policies by African Regional Organizations and Their Adoption in Zambia and Kenya (8 August 2025). https://www.developlocal.org
101. Brookings Institution, Fostering an Inclusive Digital Economy in Africa (Washington DC: Brookings Institution, 2024).
102. Key Informant Interview, Technology and Human Rights Practitioner, Amnesty International Kenya, Nairobi, August 2025 (on file with authors).
103. Key Informant Interview, op. cit. (Amnesty International Kenya).
104. Key Informant Interview, Independent Advocate and Legal Informatics Specialist, High Court of Kenya, August 2025 (on file with authors).
105. Key Informant Interview, Senior Advocacy Official, Bloggers Association of Kenya (BAKE), Nairobi, August 2025 (on file with authors). An independent legal expert separately confirmed the BAKE appeal is ongoing.
106. Key Informant Interview, Senior Representative, Data Protection Governance Society of Kenya (DPGSK), Nairobi, August 2025 (on file with authors).
107. A.M. Laibuta, Adequacy of Data Protection Regulation in Kenya (Doctoral dissertation, University of the Witwatersrand, 2023). Wits Institutional Repository.
108. M. Maseko, op. cit. (see endnote 9).
109. F. Sucker and A. Beyleveld, op. cit. (see endnote 15).
110. J.C.S. Gummadi, op. cit. (see endnote 14).
111. N. Mishra and K. Kugler, op. cit. (see endnote 16).
112. R. Kakungulu-Mayambala and S. Rukundo, op. cit. (see endnote 46).
113. Access Now, 'Tunisia: Decree 54 Uses Cybercrime to Target Dissent', Access Now Reports [Preprint], 2023. https://www.accessnow.org
114. R.Y. Kudozia et al., 'Cloud Readiness and Digital Infrastructure Gaps in Ghana', International Journal of Research and Scientific Innovation, 12(11), 2025, p. 2053. doi:10.51244/ijrsi.2025.12110180.
115. T.H. Sime, op. cit. (see endnote 12).
116. J.P. Nsengimana, 'Reflections upon Periclitations in Privacy: Perspectives from Rwanda's Digital Transformation', Health and Technology, 7(4), 2017, p. 377.
117. Key Informant Interview, Regulatory Affairs Official, Media Council of Kenya (MCK), Nairobi, August 2025 (on file with authors).
118. Key Informant Interview, Senior Representative, Data Protection Governance Society of Kenya (DPGSK), Nairobi, August 2025 (on file with authors).

Endnotes

119. Key Informant Interview, Research Consultant (Law, Technology and Digital Rights), East Africa, August 2025 (on file with authors).
120. Key Informant Interview, Senior Official, Regulatory Affairs Division, Communications Authority of Kenya (CA), Nairobi, August 2025 (on file with authors).
121. H. Abdullateef, 'Cybersecurity in Africa: Opportunities and Challenges in Emerging Markets', Zenodo [Preprint], 2025. Accessed 13 March 2026. doi:10.5281/zenodo.18163432
122. B. Ndemo, 'The Paradigm Shift: Disruption, Creativity, and Innovation in Kenya', in Palgrave Macmillan UK eBooks (Palgrave Macmillan, 2016). doi:10.1057/978-1-137-57878-5_1.
123. Communications Authority of Kenya (CA), Fourth Quarter Sector Statistics Report for the Financial Year 2024/2025 (Nairobi: CA, 2025).
124. A.S. Cruz and F.J. Mafambissa, 'Industries without Smokestacks', in Oxford University Press eBooks (Oxford: OUP, 2018). doi:10.1093/oso/9780198821885.003.0012.
125. J. Aurazo and F. Gasmi, 'Digital Payment Systems in Emerging Economies: Lessons from Kenya, India, Brazil, and Peru', Information Economics and Policy, 69, 2024, p. 101113. doi:10.1016/j.infoecopol.2024.101113.
126. Ushahidi, Platform Overview (2025). Accessed 20 November 2025. https://www.ushahidi.com/
127. iHub, About Us (2025). Accessed 20 November 2025. https://ihub.co.ke/about
128. B.O. Ongeri et al., International Trade and Recovery Strategies in Kenya in the Context of COVID-19 (AOSIS, 2022). doi:10.4102/aosis.2022.bk391.
129. United Nations General Assembly, The International Covenant on Civil and Political Rights (ICCPR), Treaty Series, vol. 999, p. 171, 1966. https://archive.org/details/3ae6b36c0
130. O.M. Sibanda, 'Towards a More Effective and Coordinated Response by the African Union on Children's Privacy Online in Africa', African Human Rights Yearbook / Annuaire Africain des Droits de l'Homme, 6(1), 2023. doi:10.29053/2523-1367/2022/v6a7.
131. M.M. Diallo, 'The Digital Economy in the Senegalese Territory: Observation and Analysis from the City of Dakar', HAL [Preprint], 2023. Accessed March 2026. https://hal.science/tel-04371634
132. C. Sall, 'Analysis of Cyber Incidents in Senegal from 2005 to 2023', The African Journal of Information and Communication (AJIC), 34, 2024, p. 1. doi:10.23962/ajic.i34.17851.
133. M.W. Owusu-Asante et al., 'Assessment of the Effectiveness and Efficiency of the ECOWAS Medicines Regulatory Harmonization Initiative by the Pharmaceutical Industry', Frontiers in Pharmacology, 14, 2023. doi:10.3389/fphar.2023.1184108.
134. Ministry of Communications and Digitalisation, Data Protection Commission: Brief History (Accra, 2025). Accessed 20 November 2025. https://moc.gov.gh/dpc/
135. Cybil Portal, 'Ghana — Cyber Security Authority (CSA): Her CyberTracks' (2025). Accessed 20 November 2025. https://cybilportal.org
136. e-Crime Bureau, '51 Cybersecurity Service Providers Certified by CSA', Accra, 11 July 2024.
137. K. Ggombe and R. Newfarmer, Rwanda: From Devastation to Services-First Transformation, UNU-WIDER Working Paper Series (Helsinki: UNU-WIDER, 2017). doi:10.35188/unu-wider/2017/308-0.
138. J.P. Nsengimana, op. cit. (see endnote 116).
139. S. Sangwa and E. Ekosse, 'Data Privacy in the Digital Economy Agreement (DEA): Balancing Economic Growth with Individual Rights in Rwanda', SSRN Electronic Journal [Preprint], 2025. doi:10.2139/ssrn.5663130.
140. Rwanda Information Society Authority (RISA), 'RISA CEO Highlights Rwanda's AI Policy at MWC Kigali 2025' (2025). Accessed 20 November 2025. https://www.risa.gov.rw
141. The Future Society, 'Cabinet of Rwanda Approves National AI Policy' (2023). Accessed 20 November 2025. https://thefuturesociety.org
142. B. Alex, J. Nafuna and D.P. Mirembe, 'The Role of Mobile and Social Media Services in Enhancing Freedom of Expression: Opportunities, Challenges, and Prospects for Local Platform Development in Uganda's Digital Ecosystem', arXiv [Preprint], 2025.
143. S. Bonaventure et al., 'Understanding Data Governance Policies and Practices Among Public and Private Stakeholders in Uganda: A Case of the Economic and Labour Sector', ResearchGate [Preprint], 2023. doi:10.13140/rg.2.2.29709.10729.
144. Library of Congress, 'Uganda: Computer Misuse (Amendment) Act Enacted', Washington DC (2023). Accessed 20 November 2025. https://www.loc.gov

Endnotes

145. Nucamp, 'Getting a Job in Tech in Tunisia in 2025: The Complete Guide' (2025). Accessed 20 November 2025. https://www.nucamp.co
146. Lucidity Insights, 'Tunisia Startup Ecosystem: 5th in MENA 2025' (2025). Accessed 20 November 2025. https://lucidityinsights.com
147. J. Bryant, 'Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights' (University of Vienna, 2020). https://othes.univie.ac.at/62171/
148. Central Bank of Kenya (CBK), 2024 FinAccess Household Survey (Nairobi: CBK, 2024).
149. Open Institute, A Study of National and Sub-National Data Practices in Kenya (Nairobi: Restored Data Rights Africa, 2021).
150. ODPC, Enforcement Determinations (Nairobi: ODPC, 2025). https://www.odpc.go.ke
151. Digital Cooperation Organization (DCO), op. cit. (see endnote 69).
152. GhanaFact, op. cit. (see endnote 64).
153. Author, 'Post-Ratification Impacts of the Malabo Convention in Tunisia', European Journal of International Law, 34(1), 2023, p. 89. [Author details withheld in source.]
154. Author, 'Tunisia's Cybersecurity Framework: Balancing Rights and Security Post-Arab Spring', MENA Policy Journal, 29(2), 2025, p. 112. [Author details withheld in source.]
155. Author, 'Rwanda's Digital Leap: Balancing Innovation and Rights in Cybersecurity', Journal of African Policy Studies, 31(1), 2025, p. 45. [Author details withheld in source.]
156. Author, 'Digital Governance in Rwanda', African Studies Review, 67(3), 2024, p. 210. [Author details withheld in source.]
157. Author, 'Cybersecurity in Ghana', Journal of African Law, 68(2), 2024, p. 145. [Author details withheld in source.]
158. African Journal of Privacy and Data Protection, 1, 2024. doi:10.29053/ajpdp.v1.
159. ODPC, op. cit. (see endnote 150).
160. Senior Representative, Data Protection Governance Society of Kenya (DPGSK). Correspondence with authors. Key Informant Interview, Nairobi, August 2025 (on file with authors).
161. Technology and Human Rights Practitioner, Amnesty International Kenya. Correspondence with authors. Key Informant Interview, Nairobi, August 2025 (on file with authors).
162. Independent Advocate and Legal Informatics Specialist, High Court of Kenya. Correspondence with authors. Key Informant Interview, August 2025 (on file with authors).
163. Senior Advocacy Official, Bloggers Association of Kenya (BAKE). Correspondence with authors. Key Informant Interview, Nairobi, August 2025 (on file with authors).
164. BAKE, 'Court of Appeal Declares Section 22 and 23 of Cybercrimes Act as Unconstitutional', Bloggers Association of Kenya, 6 March 2026. https://blog.bake.co.ke/2026/03/06/court-of-appeal-declares-section-22-23-of-cybercrimes-act-as-unconstitutional/ The appeal was brought by BAKE, ARTICLE 19 Eastern Africa, the Kenya Union of Journalists (KUJ), and the Law Society of Kenya (LSK). Justices Patrick Kiage, Aggrey Muchelule, and Weldon Korir struck down ss 22 and 23 of the Computer Misuse and Cybercrimes Act 2018 as unconstitutional.
165. BAKE, 'Section 22 and 23 Scrapped Off, What Next for Free Speech?', Bloggers Association of Kenya, 10 March 2026. https://blog.bake.co.ke/2026/03/10/section-22-and-23-scrapped-off-what-next-for-free-speech/ Sections 48-53 (surveillance with judicial warrant) and section 27 (cyber harassment) were upheld; petitioners are reviewing further legal avenues.
166. BAKE, Computer Misuse and Cybercrimes Act Court of Appeal Judgment Summary, Bloggers Association of Kenya, 6 March 2026. https://blog.bake.co.ke/2026/03/06/computer-misuse-and-cybercrimes-act-court-of-appeal-judgment-summary/ See also: Court of Appeal Judgment in the Computer Misuse and Cybercrimes Act Case (full text). http://blog.bake.co.ke/wp-content/uploads/2026/03/Cybercrimes-Appeal-Case-Judgement-2026.pdf
167. J. Onyeagoro, 'Kenya and Rwanda Central Banks Sign MoU for Cross-Border Payment Licensing', TechAfrica News, 13 March 2026. https://techafricanews.com/2026/03/13/kenya-and-rwanda-central-banks-sign-mou-for-cross-border-payment-licensing/ The Central Bank of Kenya (CBK) and the National Bank of Rwanda (NBR) signed the MoU on 11 March 2026,

Endnotes

establishing a Licence Passporting Framework for Payment Service Providers aligned with the EAC Cross-Border Payment System Masterplan.

168. A. Umutesi, 'What Rwanda-Kenya Fintech Deal Means for Companies', The New Times, 13 March 2026. https://www.newtimes.co.rw/article/34041/news/technology/what-rwanda-kenya-fintech-deal-means-for-companies Signed by Rwanda National Bank Governor Soraya Hakuziyaremye and Gerald Nyaoma, Deputy Governor of the CBK.

169. CBK Gives Nod to Phone Number Masking in M-Pesa Transactions, Business Daily Africa, March 2026. https://www.businessdailyafrica.com/bd/corporate/technology/cbk-gives-nod-to-phone-number-masking-in-m-pesa-transactions-5376242 The CBK letter to Safaricom dated 27 February 2026 approved implementation of data minimisation for peer-to-peer transactions; extension to merchant (Paybill/Till) transactions to follow.

170. CBK Approves M-Pesa Phone Number Masking to Boost Privacy and Stop Merchant Spam, HapaKenya, 9 March 2026. https://hapakenya.com/2026/03/09/cbk-approves-m-pesa-phone-number-masking-to-boost-privacy-stop-merchant-spam/ Under the previous system, a customer's full name and phone number were transmitted to merchants on every Lipa na M-Pesa payment, enabling data harvesting for unsolicited marketing. The masking feature aligns Safaricom with DPA 2019 section 25 (data minimisation).

171. E.P. Kenyanito, 'Africa Moves Towards a Common Cyber Security Legal Framework', Access Now, 2 June 2014. https://www.accessnow.org/africa-moves-towards-a-common-cyber-security-legal-framework/ One of the earliest civil society analyses of the AU Convention prior to its adoption at the June 2014 AU Summit. Written during Kenyanito's tenure as Sub-Saharan Africa Policy Analyst at Access Now (March 2014–December 2016).

172. E.P. Kenyanito, 'African Union Adopts Framework on Cyber Security and Data Protection', Access Now, 22 August 2014. https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/ Published immediately following the AU Assembly's adoption of the Convention at Malabo, Equatorial Guinea. Written during Kenyanito's tenure as Sub-Saharan Africa Policy Analyst at Access Now.

173. E.P. Kenyanito, 'Emerging Threats in Cybersecurity and Data Protection Legislation in African Union Countries', Access Now, 13 February 2015. https://www.accessnow.org/emerging-threats-in-cybersecurity-data-legislation-in-africa-union/ An early post-adoption analysis of implementation risks and rights concerns arising from the Convention. Written during Kenyanito's tenure as Sub-Saharan Africa Policy Analyst at Access Now.

174. E.P. Kenyanito, 'Access Now Brief: How African Countries Can Shape Cybercrime Laws that Protect Rights', Access Now, 21 December 2016. https://www.accessnow.org/access-now-brief-african-countries-can-shape-cybercrime-laws-protect-rights/ Companion advocacy piece to the December 2016 Room for Improvement report. Written during Kenyanito's tenure as Sub-Saharan Africa Policy Analyst at Access Now.

175. Republic of Kenya, Mutual Legal Assistance Act (No. 36 of 2011) (Nairobi: Government Printer, 2011). The Office of the Attorney-General is designated the Central Authority (section 5). Operates on the principle of mutuality and reciprocity; covers criminal matters generally but has no cyber-specific provisions.

176. Republic of Kenya, Foreign Judgments (Reciprocal Enforcement) Act (Cap 43 of the Laws of Kenya) (Nairobi: Government Printer, 1984, as amended 2018, revised 2022). Kenya has reciprocal arrangements with eight countries only: Australia, Malawi, Seychelles, Tanzania, Uganda, Zambia, the United Kingdom, and Rwanda. The Act covers civil money judgments only and does not extend to criminal or administrative enforcement.

177. Republic of Kenya, Extradition (Contiguous and Foreign Countries) Act (Cap 76) (Nairobi: Government Printer, as amended); Republic of Kenya, Extradition (Commonwealth Countries) Act (Cap 77) (Nairobi: Government Printer, as amended). Of the 20 Malabo ratifiers, Commonwealth members include Ghana, Rwanda, Zambia, Mozambique, Namibia, and Mauritius. None have cybercrime-specific extradition arrangements with Kenya. Malabo Article 30 would, upon Kenya's ratification, provide the treaty basis for cybercrime-specific extradition between Kenya and all Malabo State

Endnotes

Parties where the double-criminality requirement is met.

178. International Telecommunication Union (ITU), Global Cybersecurity Index 2024 (Geneva: ITU, September 2024). Kenya: 98.59 (Tier 1); Ghana: 99.27 (Tier 1); Rwanda: 98.08 (Tier 1); Mauritius: 100.0 (Tier 1); Uganda: 82.94 (Tier 3); Tunisia: 82.00 (Tier 3). In Africa, role-modelling countries (Tier 1) are Ghana, Kenya, Mauritius, Rwanda, Tanzania, Egypt, and Morocco.
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

179. World Bank, World Development Indicators 2024: Internet Users (% of population) — Kenya: 34.98% (2024). Source: ITU DataHub, compiled in World Bank WDI.
https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=KE See also: World Bank Kenya Digital Economy Acceleration Project (KDEAP), Phase 1, US$390 million, effective February 2024.
https://projects.worldbank.org/en/projects-operations/project-detail/P170941

180. GSMA, Mobile Economy Africa 2025 (London: GSMA Intelligence, 2025). Mobile technologies generated 7.7% of Africa’s GDP (US$220 billion) in 2024; 416 million mobile internet users (28% penetration).
https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/africa/

181. GSMA, Driving Digital Transformation of the Economy in Kenya (London: GSMA, October 2024). Report commissioned with Through Line Advisors. Provides country-level analysis of digitalization’s economic impact with World Bank WDI and GSMA Intelligence data.
https://www.gsma.com/about-us/regions/sub-saharan-africa/wp-content/uploads/2024/10/KENYA-DIGITAL-ECONOMY-REPORT-17TH-OCTOBER-V2.pdf

182. International Telecommunication Union (ITU), ICT Regulatory Tracker 2024 (Geneva: ITU, 2024). Kenya ranked #1 in Africa and #20 globally. The Tracker assesses regulatory environments across six benchmarks: national digital policy agenda, regulatory capacity, good governance, legal instruments for ICT/telecommunications, digital markets, and ICT competition.
https://datahub.itu.int/data/?e=DMA&i=90014

183. Serianu Africa, Africa Cybersecurity Report 2024 (Nairobi: Serianu, 2024). Estimated cybercrime losses for Africa reached US$10 billion in 2023, rising to an estimated US$13–16 billion in 2024. Kenya-specific estimates from Communications Authority of Kenya, Cybersecurity Report Q1 2025/2026 (Nairobi: CA Kenya, 2025): 2.54 billion threat events, KSh 29.9 billion estimated losses.

184. International Telecommunication Union (ITU), Global Cybersecurity Index 2014 (Geneva: ITU/ABI Research, 2014). First edition of the GCI, conducted in 2013–2014 in partnership with ABI Research. Used a 0–1 simple average methodology, not directly comparable to later editions. Kenya: 0.338; Ghana: 0.319; Rwanda: 0.156; Senegal: 0.269; Uganda: 0.175; Tunisia: 0.444.
https://www.itu.int/pub/D-STR-GCI.01-2014

185. International Telecommunication Union (ITU), Global Cybersecurity Index 2017 (Geneva: ITU, 2017). Second edition of the GCI, using a weighted-factor methodology (not comparable to 2014). Scores for the six comparator countries drawn from: bizcommunity.africa, 'Top 10 African Countries Committed to Cyber Security', 12 July 2017. Kenya: 0.574 (#45 globally); Rwanda: 0.602 (#36); Ghana: 0.569 (#46); Senegal: 0.43; Uganda: 0.392; Tunisia: 0.460.
https://nsarchive.gwu.edu/sites/default/files/documents/3897090/International-Telecommunication-Union-Global.pdf

186. World Bank, World Development Indicators: Individuals Using the Internet (% of Population). Indicator IT.NET.USER.ZS (Washington DC: World Bank/ITU, annual). Historical series 2013–2023 for Kenya, Ghana, Rwanda, Senegal, Uganda, and Tunisia. Accessed via World Bank Data portal. Kenya 2019 figure (22.7%) verified against: Kenya Housing Survey, cited in statskenya.co.ke; Kenya 2021 (38.25%): TheGlobalEconomy.com citing World Bank update.
https://data.worldbank.org/indicator/IT.NET.USER.ZS

187. GSMA, Mobile Economy Sub-Saharan Africa: Annual Reports 2018–2025 (London: GSMA Intelligence, 2018–2025). GDP contribution data: 2022 — 8.1% = $170 billion (GSMA Mobile for Development blog, 2023); 2023 — 7% = $140 billion (GSMA Mobile Economy Sub-Saharan Africa 2024, 7 November 2024); 2024 — 7.7% = $220 billion (GSMA Mobile Economy Africa 2025, all Africa). Mobile internet users 2013–2024: GSMA Intelligence historical data. Note: 2024 figure is all Africa; 2013–2023 figures are Sub-Saharan Africa.
https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/africa/

Bibliography

Abdullateef, H. (2025). 'Cybersecurity in Africa: Opportunities and Challenges in Emerging Markets'. Zenodo [Preprint]. doi:10.5281/zenodo.18163432 Accessed 13 March 2026.

Access Now. (2016). Room for Improvement: A Review of the African Union Convention on Cyber Security and Personal Data Protection. Washington DC: Access Now. https://www.accessnow.org

Access Now. (2023). 'Tunisia: Decree 54 Uses Cybercrime to Target Dissent'. Access Now Reports [Preprint]. https://www.accessnow.org

Access Now. (2024). Tunisia: Data Protection Law Reform Must Prioritize Human Rights. https://www.accessnow.org Accessed 20 November 2025.

African Journal of Privacy and Data Protection, 1, 2024. doi:10.29053/ajpdp.v1.

African Researchers Magazine. (2025). 'The Malabo Convention: Africa's Cybersecurity and Data Protection Framework Explained'. African Researchers Magazine [Preprint]. Accessed 20 November 2025.

African Union (AU). (2014). African Union Convention on Cyber Security and Personal Data Protection. Addis Ababa: AU. https://au.int/sites/default/files/treaties/29560-treaty-0048_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

African Union (AU). (2022). Malabo Roadmap. Addis Ababa: AU.

African Union (AU). (2024). Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade. Addis Ababa: AU.

African Union (AU). (2024). Status List: African Union Convention on Cyber Security and Personal Data Protection (as at 8 July 2024). Addis Ababa: AU. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection Accessed 11 September 2025.

Alex, B., Nafuna, J. and Mirembe, D.P. (2025). 'The Role of Mobile and Social Media Services in Enhancing Freedom of Expression: Opportunities, Challenges, and Prospects for Local Platform Development in Uganda's Digital Ecosystem'. arXiv [Preprint].

Amnesty International. (2025). Tunisia 2024: The State of the World's Human Rights. https://www.amnesty.org Accessed 20 November 2025.

Amnesty International Kenya. (2025). 5 Years On: DPA Perspectives. Nairobi: Amnesty International.

Asaka, J.O. and Oluoko-Odingo, A.A. (2022). 'Introduction', in Routledge eBooks. Routledge.

Aurazo, J. and Gasmi, F. (2024). 'Digital Payment Systems in Emerging Economies: Lessons from Kenya, India, Brazil, and Peru'. Information Economics and Policy, 69, p. 101113. doi:10.1016/j.infoecopol.2024.101113.

Aynaoui, K.E., Jaïdi, L. and Zaoui, A. (2022). Digitalise to Industrialise. Routledge eBooks. doi:10.4324/9781003274322-7.

Ball, K.M. (2017). 'African Union Convention on Cyber Security and Personal Data Protection'. International Legal Materials, 56(1), p. 164. doi:10.1017/ilm.2016.3.

Bloggers Association of Kenya (BAKE) v Attorney General [2018] KEHC 9469 (KLR), 29 May 2018 (Mwita J., conservatory orders); Bloggers Association of Kenya (BAKE) v Attorney General & 3 others; Article 19 East Africa & another (Interested Parties) [2020] KEHC 7924 (KLR) (substantive dismissal); reversed in part by Bloggers Association of Kenya (BAKE) v Attorney General & 6 others (Civil Appeal 197 of 2020) [2026] KECA 430 (KLR), 6 March 2026.

Bloggers Association of Kenya (BAKE). (2026a). 'Court of Appeal Declares Section 22 and 23 of Cybercrimes Act as Unconstitutional'. Nairobi: BAKE, 6 March 2026. https://blog.bake.co.ke/2026/03/06/court-of-appeal-declares-section-22-23-of-cybercrimes-act-as-unconstitutional/

Bloggers Association of Kenya (BAKE). (2026b). 'Section 22 and 23 Scrapped Off, What Next for Free Speech?'. Nairobi: BAKE, 10 March 2026. https://blog.bake.co.ke/2026/03/10/section-22-and-23-scrapped-off-what-next-for-free-speech/

Bloggers Association of Kenya (BAKE). (2026c). Computer Misuse and Cybercrimes Act: Court of Appeal Judgment Summary. Nairobi: BAKE, 6 March 2026. https://blog.bake.co.ke/2026/03/06/computer-misuse-and-cybercrimes-act-court-of-appeal-judgment-summary/

Bibliography

Bonaventure, S. et al. (2023). 'Understanding Data Governance Policies and Practices Among Public and Private Stakeholders in Uganda: A Case of the Economic and Labour Sector'. ResearchGate [Preprint]. doi:10.13140/rg.2.2.29709.10729.

African Union. (2024). Protocol to the Agreement Establishing the African Continental Free Trade Area on Digital Trade. Addis Ababa: African Union, 17–18 February 2024.

Bouke, M.A. et al. (2023). 'African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions'. arXiv. doi:10.48550/arxiv.2307.01966.

Brookings Institution. (2024). Fostering an Inclusive Digital Economy in Africa. Washington DC: Brookings Institution.

Business Daily Africa. (2026). 'CBK Gives Nod to Phone Number Masking in M-Pesa Transactions'. Business Daily Africa, March 2026. https://www.businessdailyafrica.com/bd/corporate/technology/cbk-gives-nod-to-phone-number-masking-in-m-pesa-transactions-5376242

Bryant, J. (2020). 'Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights'. University of Vienna. https://othes.univie.ac.at/62171/

Carnegie Endowment for International Peace. (2023). 'Continental Cyber Security Policymaking: Implications of the Entry into Force of the Malabo Convention for Digital Financial Systems in Africa'. https://carnegieendowment.org Accessed 20 November 2025.

Center for Strategic and International Studies (CSIS). (2021). Digital Africa: Leveling Up through Governance and Trade. Washington DC: CSIS.

Central Bank of Kenya (CBK). (2024a). 2024 FinAccess Household Survey. Nairobi: CBK.

Central Bank of Kenya (CBK). (2024b). Financial Inclusion Report 2024. Nairobi: CBK.

Centre for International Governance Innovation (CIGI). (2023). Digital Sovereignty in Africa. Waterloo: CIGI.

Chatham House. (2024). 'The AU Took Important Action on Cybersecurity at Its 2024 Summit'. 23 February 2024. https://www.chathamhouse.org Accessed 20 November 2025.

Chatham House. (2025). 'The AU Can Help African Countries Adopt the UN Cybercrime Convention'. 31 October 2025. https://www.chathamhouse.org Accessed 20 November 2025.

CIPESA. (n.d.). Privacy and Data Protection in the Digital Era. Kampala: CIPESA. https://cipesa.org

Commission de Protection des Données Personnelles (CDP). (2024). Annual Report 2024. Dakar: CDP. https://www.cdp.sn

Commission de Protection des Données Personnelles (CDP). (2025). Avis Trimestriels. Dakar: CDP. https://www.cdp.sn Accessed 20 November 2025.

Committee to Protect Journalists (CPJ). (2025). 'The Law Powering Tunisia's Crackdown on the Press'. 19 December 2025. https://cpj.org Accessed 26 January 2026.

Communications Authority of Kenya (CA). (2025a). Cyber Security Report Q3 2025/2026. Nairobi: CA.

Communications Authority of Kenya (CA). (2025b). Fourth Quarter Sector Statistics Report for the Financial Year 2024/2025. Nairobi: CA.

Communications Authority of Kenya (CA). (2025c). KE-CIRT/CC Reports. Nairobi: CA.

Cruz, A.S. and Mafambissa, F.J. (2018). 'Industries without Smokestacks', in Oxford University Press eBooks. Oxford: OUP. doi:10.1093/oso/9780198821885.003.0012.

Cyber Security Authority (CSA). (2024). Press Release: Licensing and Accreditation Post-Deadline Enforcement. Accra: CSA.

Cybersecurity Ventures. (2025). Cybercrime Magazine Annual Report 2025. Sausalito: Cybersecurity Ventures.

Cybil Portal. (2025). 'Ghana — Cyber Security Authority (CSA): Her CyberTracks'. https://cybilportal.org Accessed 20 November 2025.

Bibliography

Data Protection Commission (DPC). (2024). Annual Report 2024. Accra: DPC. https://moc.gov.gh/dpc/

Data Protection Office (DPO). (2024a). Annual Report 2024. Kigali: DPO. https://dpo.gov.rw

Data Protection Office (DPO). (2024b). Guidance on Data Protection Officer Designation. Kigali: DPO. https://dpo.gov.rw Accessed 20 November 2025.

Develop Local. (2025). Digital Data Rights Policies by African Regional Organizations and Their Adoption in Zambia and Kenya. https://www.developlocal.org

Diallo, M.M. (2023). 'The Digital Economy in the Senegalese Territory: Observation and Analysis from the City of Dakar'. HAL [Preprint]. https://hal.science/tel-04371634 Accessed March 2026.

Digital Cooperation Organization (DCO). (2025). Rwanda: Digital Economy Report. Riyadh: DCO. https://dco.org

Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information (DCSSI). (2025). Missions. https://stcc-ssi.sn/mission/ Accessed 20 November 2025.

e-Crime Bureau. (2024). '51 Cybersecurity Service Providers Certified by CSA'. Accra, 11 July 2024.

Farmer, B.M. (2025). 'How Kenya Became the 'Silicon Savannah''. CBS News, 29 June 2025. https://www.cbsnews.com/news/how-kenya-became-the-silicon-savannah-60-minutes/ Accessed 26 January 2026.

Future of Privacy Forum (FPF). (2024). RECs: Towards a Continental Approach to Data Protection in Africa. Washington DC: FPF. https://fpf.org

The Future Society. (2023). 'Cabinet of Rwanda Approves National AI Policy'. https://thefuturesociety.org Accessed 20 November 2025.

Geoffrey Andare v. Attorney General [2016] eKLR. High Court of Kenya.

GhanaFact. (2025). 'Draft 2025 Cybersecurity Bill: CSA's New Functions and Police Powers'. 11 November 2025. https://ghanafact.com Accessed 20 November 2025.

Ggombe, K. and Newfarmer, R. (2017). Rwanda: From Devastation to Services-First Transformation, UNU-WIDER Working Paper Series. Helsinki: UNU-WIDER. doi:10.35188/unu-wider/2017/308-0.

Global Finance and Technology Network (GFTN). (2025). 'Ghana and Rwanda to Implement Africa's First Fintech License Passport Framework'. 3 March 2025. https://gftn.co Accessed 20 November 2025.

GSMA. (2018–2025). Mobile Economy Sub-Saharan Africa: Annual Reports 2018–2025. London: GSMA Intelligence. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/africa/

GSMA. (2025). The Mobile Economy Africa 2025. London: GSMA.

Gummadi, J.C.S. (2024). 'Cybersecurity in International Trade Agreements: A New Paradigm for Economic Diplomacy'. American Journal of Trade and Policy, 11(1), p. 39. doi:10.18034/ajtp.v11i1.738.

Human Rights Watch (HRW). (2023). Uganda: Computer Misuse Act Used to Suppress Dissent. https://www.hrw.org Accessed 20 November 2025.

Human Rights Watch (HRW). (2024). World Report 2024: Uganda. https://www.hrw.org

Human Rights Watch (HRW). (2025). Kenya: New Cybercrime Amendments. November 2025. https://www.hrw.org

IC Africa. (2025). 'Ghana's 1Q2025 Real GDP Growth Update'. June 2025. https://ic.africa Accessed 20 November 2025.

HapaKenya. (2026). 'CBK Approves M-Pesa Phone Number Masking to Boost Privacy and Stop Merchant Spam'. HapaKenya, 9 March 2026. https://hapakenya.com/2026/03/09/cbk-approves-m-pesa-phone-number-masking-to-boost-privacy-stop-merchant-spam/

Ifeanyi-Ajufo, N. (2023). 'Cyber Governance in Africa: At the Crossroads of Politics, Sovereignty and Cooperation'. Policy Design and Practice, 6(2), p. 146. doi:10.1080/25741292.2023.2199960.

iHub. (2025). About Us. https://ihub.co.ke/about Accessed 20 November 2025.

Independent Advocate and Legal Informatics Specialist, High Court of Kenya. (2025). Correspondence with authors. Key Informant Interview, August 2025 (on file with authors).

Internet Society. (2018). Personal Data Protection Guidelines for Africa. Reston: Internet Society. https://www.internetsociety.org

Bibliography

INTERPOL. (2025). Africa Cyberthreat Assessment Report 2025. Lyon: INTERPOL.

International Telecommunication Union (ITU). (2024b). ICT Development Index 2024: Measuring Digital Development. Geneva: ITU. https://www.itu.int/itu-d/reports/statistics/idi2024/

International Telecommunication Union (ITU). (2014). Global Cybersecurity Index 2014. Geneva: ITU/ABI Research. https://www.itu.int/pub/D-STR-GCI.01-2014

International Telecommunication Union (ITU). (2017). Global Cybersecurity Index 2017. Geneva: ITU. https://nsarchive.gwu.edu/sites/default/files/documents/3897090/International-Telecommunication-Union-Global.pdf

International Telecommunication Union (ITU). (2024a). Global Cybersecurity Index 2024. Geneva: ITU. https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

International Finance Corporation (IFC) and Google. (2020). e-Conomy Africa 2020. Washington DC: IFC. https://www.ifc.org/content/dam/ifc/doc/mgrt/e-conomy-africa-report.pdf

International Telecommunication Union (ITU). (2024c). ICT Regulatory Tracker 2024. Geneva: ITU. https://datahub.itu.int/data/?e=DMA&i=90014

International Telecommunication Union (ITU). (2025). Digital Development Dashboard: Africa. Geneva: ITU.

Jönsson, M. (2018). Political Economics of Gender Relations in Information and Communication Technologies in Agricultural Development: The Case of Knowledge-Based Platforms for Farmers in Kenya. HAL [Open Archive].

Kakungulu-Mayambala, R. and Rukundo, S. (2019). 'Digital Activism and Free Expression in Uganda'. African Human Rights Law Journal, 19(1). doi:10.17159/1996-2096/2019/v19n1a9.

Kenya National Bureau of Statistics (KNBS). (2025). Economic Survey 2025. Nairobi: KNBS.

KICTANet. (2023). Public Participation in ICT Policy Making. Nairobi: KICTANet.

Key Informant Interview, Independent Advocate and Legal Informatics Specialist. op. cit.

Key Informant Interview, Regulatory Affairs Official, Media Council of Kenya (MCK). (2025). Nairobi, August 2025 (on file with authors).

Key Informant Interview, Research Consultant (Law, Technology and Digital Rights). (2025). East Africa, August 2025 (on file with authors).

Key Informant Interview, Senior Advocacy Official, Bloggers Association of Kenya (BAKE). (2025). Nairobi, August 2025 (on file with authors).

Key Informant Interview, Senior Official, Communications Authority of Kenya (CA). (2025). Nairobi, August 2025 (on file with authors).

Key Informant Interview, Senior Official, Office of the Data Protection Commissioner (ODPC). (2025). Nairobi, August 2025 (on file with authors).

Key Informant Interview, Senior Representative, Data Protection Governance Society of Kenya (DPGSK). (2025). Nairobi, August 2025 (on file with authors).

Key Informant Interview, Technology and Human Rights Practitioner, Amnesty International Kenya. (2025). Nairobi, August 2025 (on file with authors).

KPMG. (2025). Uganda Tax (Amendment) Bills 2025 — Analysis. https://kpmg.com Accessed 20 November 2025.

Kugler, K. (2024). 'The AfCFTA Digital Trade Protocol'. Trade and Sustainability Review, October 2024. Ottawa: IISD. https://www.iisd.org/articles/policy-analysis/afcfta-digital-protocol

Kenyanito, E.P. (2014a). 'Africa Moves Towards a Common Cyber Security Legal Framework'. Access Now, 2 June 2014. https://www.accessnow.org/africa-moves-towards-a-common-cyber-security-legal-framework/

Kenyanito, E.P. (2014b). 'African Union Adopts Framework on Cyber Security and Data Protection'. Access Now, 22 August 2014. https://www.accessnow.org/african-union-adopts-framework-on-cyber-security-and-data-protection/

Kenyanito, E.P. (2015). 'Emerging Threats in Cybersecurity and Data Protection Legislation in African Union Countries'. Access Now, 13 February 2015. https://www.accessnow.org/emerging-threats-in-cybersecurity-data-legislation-in-africa-union/

Bibliography

Kenyanito, E.P. (2016). 'Access Now Brief: How African Countries Can Shape Cybercrime Laws that Protect Rights'. Access Now, 21 December 2016. https://www.accessnow.org/access-now-brief-african-countries-can-shape-cybercrime-laws-protect-rights/

GSMA Intelligence. (2025). Mobile Economy Africa 2025. London: GSMA Intelligence. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/africa/

GSMA. (2024). Driving Digital Transformation of the Economy in Kenya. London: GSMA (October 2024). https://www.gsma.com/newsroom/press-release/kenyas-digital-economy-to-contribute-ksh-662-billion-to-gdp-by-2028-driven-by-policy-reforms/

International Telecommunication Union. (2024). ICT Development Index 2024: Measuring Digital Development. Geneva: ITU. https://www.itu.int/itu-d/reports/statistics/idi2024/

International Telecommunication Union. (2025). ICT Regulatory Tracker 2025. Geneva: ITU. Kenya score: 93/100; #1 Africa; #20 globally. https://www.itu.int/en/ITU-D/Regulatory-Market/Pages/Regulatory-Tracker.aspx

Internet World Stats. (2024). Africa Internet Stats and Population. Kenya internet penetration: 85.2%. https://www.internetworldstats.com/af/ke.htm

World Bank. (2023). Kenya and the World Bank Group Provide a $390 Million Boost to the Digital Economy. Press Release. Washington DC: World Bank. https://www.worldbank.org/en/news/press-release/2023/04/05/kenya-afe-and-the-world-bank-group-provide-a-390-million-boost-the-digital-economy

World Bank Group. (2024). Digital Economy for Africa (DE4A) Initiative: Progress Report. Washington DC: World Bank. https://www.worldbank.org/en/programs/all-africa-digital-transformation

World Bank. (2024d). World Development Indicators 2024: Internet Users (% of Population). Washington DC: World Bank. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=KE

Kudozia, R.Y. et al. (2025). 'Cloud Readiness and Digital Infrastructure Gaps in Ghana'. International Journal of Research and Scientific Innovation, 12(11), p. 2053. doi:10.51244/ijrsi.2025.12110180.

Laibuta, A.M. (2023). Adequacy of Data Protection Regulation in Kenya. Doctoral dissertation, University of the Witwatersrand. Wits Institutional Repository.

Library of Congress. (2023). 'Uganda: Computer Misuse (Amendment) Act Enacted'. Washington DC. https://www.loc.gov Accessed 20 November 2025.

Lucidity Insights. (2025). 'Tunisia Startup Ecosystem: 5th in MENA 2025'. https://lucidityinsights.com Accessed 20 November 2025.

Maseko, M. (2024). 'Understanding Digital Rights in an Era of Digital Politics in Africa'. Digital Policy Studies, 3(1), p. 58. doi:10.36615/ba9c4567.

Ministry of Communications and Digitalisation. (2025). Data Protection Commission: Brief History. Accra. https://moc.gov.gh/dpc/ Accessed 20 November 2025.

Ministry of ICT and Innovation (MINICT). (2024). National Cybersecurity Strategy of the Republic of Rwanda 2024–2029. Kigali: MINICT.

Ministry of ICT and National Guidance. (2022). National Cybersecurity Strategy 2022–2026. Kampala: MoICT.

Ministry of ICT, Innovation and Youth Affairs. (2022). Kenya National Digital Master Plan 2022–2032. Nairobi: Republic of Kenya.

Mishra, N. and Kugler, K. (2024). 'International Community in the Global Digital Economy: A Case Study on the African Digital Trade Framework'. International and Comparative Law Quarterly, 73(4), p. 853. doi:10.1017/s0020589324000290.

Muhairwe, N. (2024). Analysing the Challenges in Enforcement of Data Protection Laws in Uganda. Master's thesis, Uganda Christian University. https://scholar.ucu.ac.ug

National Institute of Statistics of Rwanda (NISR). (2025). GDP National Accounts (First Quarter 2025). Kigali: NISR. https://www.statistics.gov.rw Accessed 20 November 2025.

Ndemo, B. (2016). 'The Paradigm Shift: Disruption, Creativity, and Innovation in Kenya', in Palgrave Macmillan UK

Bibliography

eBooks. Palgrave Macmillan. doi:10.1057/978-1-137-57878-5_1.

Ndemo, E.B. (2015). 'Political Entrepreneurialism: Reflections of a Civil Servant on the Role of Political Institutions in Technology Innovation and Diffusion in Kenya'. Stability: International Journal of Security and Development, 4(1). doi:10.5334/sta.fd.

Nsengimana, J.P. (2017). 'Reflections upon Periclitations in Privacy: Perspectives from Rwanda's Digital Transformation'. Health and Technology, 7(4), p. 377. doi:10.1007/s12553-017-0196-0.

Nucamp. (2025). 'Getting a Job in Tech in Tunisia in 2025: The Complete Guide'. https://www.nucamp.co Accessed 20 November 2025.

Office of the Data Protection Commissioner (ODPC). (2024). Strategic Plan 2023–2027. Nairobi: ODPC.

ODPC. (2025a). Enforcement Determinations. Nairobi: ODPC. https://www.odpc.go.ke

ODPC. (2025b). Kenya Undertakes Stakeholder Consultations on Accession to the Malabo Convention. Nairobi: ODPC, 8 September 2025. https://www.odpc.go.ke

ODPC. (2025c). Sector Specific Guidelines. Nairobi: ODPC, November 2025.

Ongeri, B.O. et al. (2022). International Trade and Recovery Strategies in Kenya in the Context of COVID-19. AOSIS. doi:10.4102/aosis.2022.bk391.

Onyango, C. (2025). 'Fintech Passport: Why a Ghana License Now Works in Rwanda and Vice Versa'. Finance in Africa, 5 November 2025. https://financeinafrica.com Accessed 20 November 2025.

Onyeagoro, J. (2026). 'Kenya and Rwanda Central Banks Sign MoU for Cross-Border Payment Licensing'. TechAfrica News, 13 March 2026.
https://techafricanews.com/2026/03/13/kenya-and-rwanda-central-banks-sign-mou-for-cross-border-payment-licensing/

Open Institute. (2021). A Study of National and Sub-National Data Practices in Kenya. Nairobi: Restored Data Rights Africa.

Owusu-Asante, M.W. et al. (2023). 'Assessment of the Effectiveness and Efficiency of the ECOWAS Medicines Regulatory Harmonization Initiative by the Pharmaceutical Industry'. Frontiers in Pharmacology, 14. doi:10.3389/fphar.2023.1184108.

Oxfam. (2024). ReCIPE Project Framework Document. Nairobi: Oxfam. https://www.oxfamrecipe.eu/

Oxfam in ReCIPE and Al Khatt. (2026). Policy Paper on the Legal Framework on Cybercrime in Tunisia. 20 January 2026. https://www.oxfamrecipe.eu/

Paradigm Initiative. (2022). The Malabo Roadmap: Advancing Data Protection and Cybercrime Frameworks in Africa. Data Protection Africa. https://dataprotection.africa Accessed September 2022.

Presidency of the Republic of Senegal. (2025a). New Deal Technologique: A National Ambition to Make Senegal a Leader in the Digital Economy in Africa. Dakar, 24 February 2025. https://www.presidence.sn Accessed 20 November 2025.

Presidency of the Republic of Senegal. (2025b). Senegal Signs a $10 Million Strategic Partnership with the Gates Foundation. Dakar, September 2025. https://www.presidence.sn

Regulatory Authority for Telecommunications and Posts (ARTP). (2025). Missions et Attributions. https://www.artp.sn Accessed 20 November 2025.

Republic of Ghana. (2008). Electronic Transactions Act, 2008 (Act 772). Accra: Government Printer.

Republic of Ghana. (2012). Data Protection Act, 2012 (Act 843). Accra: Government Printer.

Republic of Ghana. (2020). Cybersecurity Act, 2020 (Act 1038). Accra: Government Printer.

Republic of Ghana. (2025). Cybersecurity (Amendment) Bill 2025. Accra: Government Printer.

Republic of Kenya. Extradition (Contiguous and Foreign Countries) Act (Cap 76). Nairobi: Government Printer.

Republic of Kenya. Extradition (Commonwealth Countries) Act (Cap 77). Nairobi: Government Printer

Republic of Kenya. (1984, amended 2018, revised 2022). Foreign Judgments (Reciprocal Enforcement) Act (Cap 43). Nairobi: Government Printer. https://new.kenyalaw.org/akn/ke/act/1984/4/eng@2022-12-31

Republic of Kenya. (2008). Kenya Vision 2030: The Popular Version. Nairobi: Government Printer.

Republic of Kenya. (2011). Mutual Legal Assistance Act (No. 36 of 2011). Nairobi: Government Printer. https://www.policyvault.africa/wp-content/uploads/policy/KEN467.pdf

Bibliography

Republic of Kenya. (2018). Computer Misuse and Cybercrimes Act (Act No. 5 of 2018). Nairobi: Government Printer.

Republic of Kenya. (2019). Data Protection Act (Act No. 24 of 2019). Nairobi: Government Printer.

Republic of Kenya. (2022). Kenya National Digital Master Plan 2022–2032. Nairobi: Government Printer.

Republic of Kenya. (2023). Open Government Partnership (OGP) 5th National Action Plan 2023–2027. Nairobi: Republic of Kenya.

Republic of Kenya. (2024). Computer Misuse and Cybercrimes (Critical Information Infrastructure and Cybercrime Management) Regulations 2024. Kenya Gazette Vol. CXXVI, No. 18, 16 February 2024.

Republic of Kenya. (2025). Computer Misuse and Cybercrimes (Amendment) Act (Act No. 17 of 2025). Nairobi: Government Printer.

Republic of Rwanda. (2018). Law No. 60/2018 of 13 August 2018 on Prevention and Punishment of Cyber Crimes. Kigali: Government Printer.

Republic of Rwanda. (2020). 4th Industrial Revolution Strategy 2020–2025. Kigali: Government Printer.

Republic of Rwanda. (2021). Law No. 058/2021 of 13 October 2021 Relating to the Protection of Personal Data and Privacy. Kigali: Government Printer.

Republic of Senegal. (2008a). Law No. 2008-08 of 25 January 2008 on Electronic Transactions. Dakar: Government Printer.

Republic of Senegal. (2008b). Law No. 2008-12 of 25 January 2008 on the Protection of Personal Data. Dakar: Government Printer.

Republic of Senegal. (2016). Law No. 2016-29 of 8 November 2016 (amending the Senegalese Penal Code). Dakar: Government Printer.

Republic of Tunisia. (2004). Organic Law No. 2004-63 of 27 July 2004 on the Protection of Personal Data. Tunis: Government Printer.

Republic of Tunisia. (2022). Decree-Law No. 2022-54 of 13 September 2022. Tunis: Government Printer.

Republic of Tunisia. (2023). Decree-Law No. 2023-17 of 11 March 2023 on Cybersecurity. Tunis: Government Printer.

Republic of Uganda. (2011). Computer Misuse Act (Act No. 2 of 2011, as amended 2022). Kampala: Government Printer.

Republic of Uganda. (2019). Data Protection and Privacy Act (Act No. 9 of 2019). Kampala: Government Printer.

Rwanda Information Society Authority (RISA). (2025). 'RISA CEO Highlights Rwanda's AI Policy at MWC Kigali 2025'. https://www.risa.gov.rw Accessed 20 November 2025.

Sall, C. (2024). 'Analysis of Cyber Incidents in Senegal from 2005 to 2023'. The African Journal of Information and Communication (AJIC), 34, p. 1. doi:10.23962/ajic.i34.17851.

Sangwa, S. and Ekosse, E. (2025). 'Data Privacy in the Digital Economy Agreement (DEA): Balancing Economic Growth with Individual Rights in Rwanda'. SSRN Electronic Journal [Preprint]. doi:10.2139/ssrn.5663130.

Senior Advocacy Official, Bloggers Association of Kenya (BAKE). (2025). Correspondence with authors. Key Informant Interview, Nairobi, August 2025 (on file with authors).

Senior Official, Regulatory Affairs Division, Communications Authority of Kenya (CA). (2025). Correspondence with authors. Key Informant Interview, Nairobi, August 2025 (on file with authors).

Senior Official, Office of the Data Protection Commissioner (ODPC). (2025). Correspondence with authors. Key Informant Interview, Nairobi, August 2025 (on file with authors).

Senior Representative, Data Protection Governance Society of Kenya (DPGSK). (2025). Correspondence with authors. Key Informant Interview, Nairobi, August 2025 (on file with authors).

Serianu. (2025). Africa Cybersecurity Report — Kenya 2025. Nairobi: Serianu.

Sibanda, O.M. (2023). 'Towards a More Effective and Coordinated Response by the African Union on Children's Privacy Online in Africa'. African Human Rights Yearbook / Annuaire Africain des Droits de l'Homme, 6(1). doi:10.29053/2523-1367/2022/v6a7.

Sime, T.H. (2023). 'A Critical Reflection on African Maritime Cybersecurity Frameworks'. Scientia Militaria: South African Journal of Military Studies, 51(3). doi:10.5787/51-3-1426.

Bibliography

Soulé, F. (2025). 'Navigating the Multiplexity of Africa's Digital Partnerships amidst Global Rivalry'. Global Studies Quarterly, 5(4). doi:10.1093/isagsq/ksaf114.

Startup Genome. (2025). Tunisia — Ecosystem. https://startupgenome.com Accessed 20 November 2025.

Sucker, F. and Beyleveld, A. (2024). 'African Rules on Cross-Border Data Flows: The Significance of Regulatory Convergence and the AfCFTA Digital Trade Protocol's Potential Contribution'. SSRN Electronic Journal [Preprint]. doi:10.2139/ssrn.4741632.

Technology and Human Rights Practitioner, Amnesty International Kenya. (2025). Correspondence with authors. Key Informant Interview, Nairobi, August 2025 (on file with authors).

Uganda Bureau of Statistics (UBOS). (2025). Annual Gross Domestic Product: Fiscal Year 2024/25. Kampala: UBOS. https://www.ubos.org Accessed 20 November 2025.

Uganda Registration Services Bureau (URSB). (2025). Uganda's Data Protection Office Finds Google in Breach of Privacy. Kampala: URSB. https://ursb.go.ug Accessed 20 November 2025.

United Nations Conference on Trade and Development (UNCTAD). (2024). Data Protection Legislation Worldwide. Geneva: UNCTAD.

United Nations General Assembly. (1966). The International Covenant on Civil and Political Rights (ICCPR), Treaty Series, vol. 999, p. 171. https://archive.org/details/3ae6b36c0

Ushahidi. (2025). Platform Overview. https://www.ushahidi.com/ Accessed 20 November 2025.

U.S. International Trade Administration. (2024). 'Kenya — Digital Economy', Country Commercial Guide. https://www.trade.gov Accessed 20 November 2025.

Umutesi, A. (2026). 'What Rwanda-Kenya Fintech Deal Means for Companies'. The New Times, 13 March 2026. https://www.newtimes.co.rw/article/34041/news/technology/what-rwanda-kenya-fintech-deal-means-for-companies

Walubengo, J. and Mutemi, M. (2018). 'Treatment of Kenya's Internet Intermediaries under the Computer Misuse and Cybercrimes Act, 2018'. The African Journal of Information and Communication (AJIC), 21. doi:10.23962/10539/26114.

World Bank. (2024). Digital Economy for Africa. Washington DC: World Bank.

World Intellectual Property Organization (WIPO). (2025). Global Innovation Index 2025: Uganda Profile. Geneva: WIPO. https://www.wipo.int Accessed 20 November 2025.

World Trade Organization (WTO). (2024). Annual Report 2024. Geneva: WTO.

World Trade Organization (WTO) and World Bank. (2024). Digital Trade Needs Assessments: Kenya and Rwanda. Geneva: WTO, February 2024. https://www.wto.org/english/news_e/news24_e/dtech_24feb24_e.htm

Yusuf, B. (2023). Robust Digital Governance Frameworks in Africa. Waterloo: CIGI.