Journal of Intellectual Property and Information Technology Law
(JIPIT)

Data Governance in the Public Interest

The Journal of Intellectual Property and Information Technology Law (JIPIT) is a law journal managed by the Centre for Intellectual Property and Information Technology Law (CIPIT) and hosted under the Strathmore University Press (SUP). CIPIT is a research centre based at Strathmore University. Over the years, CIPIT has positioned itself as a thought leader in the evolving fields of law, technology, and innovation across Africa. The Centre conducts evidence-based research on issues at the intersection of law, technology, and innovation in Africa. Our work spans across key thematic areas including Intellectual Property, Artificial Intelligence, Data Governance and Policy, Cyber Law and Policy, and Digital ID.

JIPIT was established in 2020 to provide a platform for publishing outstanding research and scholarly analyses on legal matters related to IP, ICT, and AI in the Global South. It consistently publishes peer-reviewed journal articles and commentaries annually.

Kindly access the Submission Guidelines, Style Guide, and previous Issues at: https://journal.strathmore.edu/index.php/jipit

Journal of Intellectual Property and Information Technology Law

JIPIT

Volume 6, Issue 1
August 2026

ISSN 2788-6727
DOI: 10.52907/jipit.2026

Data Governance in the Public Interest



Strathmore University
Press

Editorial Board

Editor-in-Chief
Dr Melissa Omino

Issue Editor
Collins C. Okoh

Production Editor
Chebet Koros

Associate Editor
Cynthia Nzuki

Associate Editor
Joshua Kitili

Editorial Assistants

Anthony Mburu
Esther Onyango
Grace Njenga
Michael Olach
Nelly Irungu
Zaiba Noorani







This Special Issue arises from the Data Privacy and Governance Society of Kenya (DPGSK) Annual Conference and Research Day, organized in collaboration with Amnesty International and CIPIT. We appreciate these organizations for their support.

This publication was facilitated by a grant from the Hewlett Foundation.

Typesetting and artwork
John Agutu,
Email: agutujo@yahoo.com

Printed by
P.O. Box 44466 – 00100 GPO Nairobi

Table of Contents

Editorial 7

Foreword 11

Posthumous Data Privacy in Kenya
Timothy Samson Omondi Ayuo 15

Fortifying the Digital Frontier: An Analysis of Legal and Technical Frameworks for Data Systems Resilience in Kenya
Martin Mungai 59

Who Owns the Face? Reimagining Image Rights in Kenya Through African Personhood
Renee Tikolo 101

Governing AI-Generated Likeness: African Legal and Philosophical Frameworks
Onyinyechi Cynthia Igodo 169

Constitutional Governance and Digital Identity Transformation in Kenya
Stephen Larzen Juma 263

Data Rights and Participatory Governance: An Analysis of Health Data Governance in Kenya
Silvia W. Mwangi & Maria N. Bosita 299

JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 5, Issue 1 (2025) p.7-10
DOI: https:doi.org/10.52907/jipit.2026.652

Editorial

I am pleased to present the sixth volume of the Journal of Intellectual Property and Information Technology Law (JIPIT). This Special Issue, themed '*Data Governance in the Public Interest*', affirms our continued commitment to publishing rigorous, policy-relevant scholarship on data protection, artificial intelligence (AI), intellectual property (IP), and ICT law within the Global South. It also reinforces our enduring mission to nurture and amplify African-centered legal research that speaks directly to the continent's most pressing digital governance challenges.

This Edition is a post-event publication arising from the Data Protection and Governance Society of Kenya (DPGSK) Annual Conference and Research Day, organized in collaboration with Amnesty International and the Centre for Intellectual Property and Information Technology Law (CIPIT) at Strathmore University. The conference brought together scholars, practitioners, regulators, and civil society actors to examine contemporary data protection challenges facing Kenya and the broader Global South. The six papers in this Issue, spanning posthumous data rights, cyber resilience, image rights grounded in African personhood, AI-generated likeness governance, digital identity constitutionalism, and participatory health data governance, address these challenges from distinct yet complementary vantage points. Together, they paint a nuanced portrait of where Kenya, and Africa more broadly, stands in its ongoing effort to build data protection regimes that are both globally informed and locally responsive. In curating this Volume from the conference's scholarly output, JIPIT continues a tradition that has proven fruitful in prior editions:

translating the intellectual energy of live academic dialogue into peer-reviewed contributions of lasting value; influencing policies and yielding practical results across the breadth of the Global South for both the present and future generations.

Introducing the Issue is Timothy S. O. Ayuo in *'Posthumous Data Privacy in Kenya'*. Ayuo examines the legal gap in Kenya's Data Protection Act, 2019, which safeguards the rights of living natural persons but remains silent on the status of personal data after death. Guided by the dignity theory and autonomy theory, and drawing on comparative jurisprudence from Rwanda and China, Ayuo argues for the necessity of legal recognition of posthumous privacy in compliance with constitutional rights to privacy and dignity under Articles 28 and 31 of the Constitution of Kenya, 2010.

This is ably followed by Martin Mungai in *'Fortifying the Digital Frontier: An Analysis of Legal and Technical Frameworks for Data Systems Resilience in Kenya'*. Mungai argues that Kenya's data resilience deficit has been persistently misdiagnosed as a gap in data protection law when it is, in fact, a gap in institutional construction. Although Kenya possesses a prescriptive resilience regime under the Computer Misuse and Cybercrimes Act (2018) and its 2024 Regulations, legal obligations remain unrealized. Drawing on incidents including the 2023 eCitizen outage and recurring M-Pesa disruptions, Mungai makes three-phased recommendations to address the challenge.

Next, in *'Who Owns the Face? Reimagining Image Rights in Kenya Through African Personhood',* Renee Tikolo contends that images of African individuals are carriers of relational identity and personal embeddedness, not merely data points or creative property. At stake, Tikolo argues, is not merely ownership but the power to determine how African stories are represented and valued. Drawing on the blended model of personhood, Tikolo demonstrates that existing privacy, copyright, and data protection frameworks cannot recognize the full dimension of harm when African images are extracted and commercialized. Tikolo proposes reforms at national, continental, and internation-

al levels to ensure proper attribution, fair benefit-sharing, and cross-border accountability.

Shifting focus to AI governance, Onyinyechi C. Igodo also examines likeness and communal cultural imagery in *'Governing AI-Generated Likeness: African Legal and Philosophical Frameworks'*. Through comparative analysis of South Africa, Nigeria, and Kenya, Igodo demonstrates that generative AI collapses two traditionally distinct categories, individual likeness rights and communal cultural imagery, by generating identifiable persons and culturally significant contexts. Drawing on Ubuntu and broader African philosophies of relational personhood, the author proposes a hybrid governance framework integrating personality rights, cultural heritage protections, collective consent mechanisms, and indigenous data sovereignty.

In *'Constitutional Governance and Digital Identity Transformation in Kenya',* Stephen L. Juma argues that Kenya's digital identity reforms, from Huduma Namba to Maisha Namba, have been treated as technical projects rather than governance infrastructures shaping who is recognized by the state and who can participate in civic life. Juma demonstrates that systems designed to broaden access are generating new forms of exclusion, particularly for undocumented youth and marginalized populations, with judicial interventions repeatedly exposing gaps in Data Protection Impact Assessments. Comparing Kenya's experience with Venezuela's politicized Carnet de la Patria and Estonia's rights-based e-identity model, Juma proposes reforms to ensure digital identity serves democratic governance rather than exclusion or surveillance.

Concluding the Issue, Silvia W. Mwangi and Maria N. Bosita investigate Kenya's health data governance framework in *'Data Rights and Participatory Governance: An Analysis of Health Data Governance in Kenya'*. Focusing on the Constitution and the Digital Health Act (No. 15 of 2023), the authors argue that sustainable health data governance requires more than technical safeguards; as Kenya expands its digital health sys-

tems, governance must be matched by meaningful and continuous public participation. Drawing on the United Kingdom's data trust models, Mwangi and Bosita propose recommendations for strengthening participatory governance within Kenya's existing legal and institutional framework.

Taken together, these six papers exemplify the mission of JIPIT: scholarship that does not merely describe challenges but proposes solutions, and that does not merely observe the present but anticipates the future. This ambition is only possible through sustained collaboration. I am deeply grateful to the authors whose thoughtful contributions animate this Volume and deepen the scholarly conversation on data protection in the Global South, and equally to the peer-review editorial team and expert reviewers, whose intellectual rigor and generous engagement with the manuscripts ensured the quality and integrity of this Special Issue.

Yet collaboration does not end with publication; it extends into implementation and beyond. As the Global South's digital transformation accelerates, JIPIT stands ready to host the scholarship that will illuminate the path ahead. To regulators, practitioners, and policymakers engaging with the papers in this Issue, the invitation is to act: to translate these proposals into policy reform, institutional design, and operational practice. To scholars preparing the next wave of research, your voice belongs in the next pages. Whether you are an emerging researcher with a bold thesis or an established expert with hard-won insights, JIPIT offers a platform where rigorous ideas meet real-world impact. The future of Global South digital governance will not write itself. It will be shaped by those who step forward, and we invite you to be among them.

To have your work considered, please submit your manuscripts by visiting: https://journal.strathmore.edu/index.php/jipit/about/submissions or by writing to cipitjournal@strathmore.edu

Collins C. OKOH (FIP, CIPM, CIPP/E),
Issue Editor, JIPIT, August 2026,
Email: contact@collinsokoh.com

JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 6, Issue 1 (2026) p.11-12
DOI: https:doi.org/10.52907/jipit.2026.653

Foreword

The papers featured in this volume began as works in progress presented at the Annual Conference and Research Day of the Data Privacy and Governance Society of Kenya, convened in partnership with CIPIT and Amnesty International Kenya on 22 October 2025.

The theme of the Research Day, 'Data Governance in the Public Interest', invited scholars to share insights, strategies, and innovations that will shape the future of responsible and effective data management in ways that promote the public good while safeguarding individual rights across Africa. Four keywords anchor the call for papers: accountability, transparency, fairness, and accessibility. Each contribution in this edition can be read as an effort to give legal and practical content to one or more of these foundational principles.

Three papers in this volume explore the contours of the data subject as currently defined by the Kenyan Data Protection Act. The Act speaks only of living natural persons and does not venture beyond that framing, leaving a significant lacuna when it comes to personal or sensitive data that pertains to deceased persons. Two of these papers engage directly with image rights: one examines African concepts of personhood and the distinct communal dimensions they bring to questions of identity and representation, while the other investigates how generative systems replicate individual likeness and communal cultural imagery, arguing for a hybrid model that distinguishes personal image rights from collective interests in cultural heritage while acknowledging the connections between the two. Read together,

these papers demonstrate that interpreting 'the person' as contemplated by Article 28 of the Constitution demands more than importing categories from other jurisdictions; it calls for legal solutions tailored to the local context.

A second group of papers addresses the question of whether public participation in data governance is merely a procedural courtesy or a substantive governance method with real consequences for rights and accountability. A health data governance analysis examines the Digital Health Act, 2023 alongside constitutional guarantees, exploring how data trusts and stewardship models can ensure that public involvement in decisions about secondary use of health data moves beyond a tick-box exercise to become a meaningful mechanism for collective oversight.

The methodological diversity on display in these papers is a strength of this collection. The papers show that authors have grappled with and interrogated a wide range of evidence, including doctrinal analysis, comparative study, and empirical inquiry, and the conclusions they reach advance the broader discourse on data governance across the Continent. We now present these papers to you in the hope that they will provoke thought, invite critique, and inspire further scholarship and better data governance.

We are grateful to the Data Privacy and Governance Society of Kenya and Amnesty International Kenya, whose partnership made the Research Day possible; to the reviewers whose careful reading strengthened every paper in these pages; and above all to the authors, who accepted the discipline of presenting unfinished work in public and returned with it improved.

Dr. Melissa Omino,
Director, Centre for Intellectual Property and Information Technology Law (CIPIT),
Strathmore University,
Nairobi, Kenya,
August 2026.

ARTICLES

JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 6, Issue 1 (2026) p.15-58
DOI: https:doi.org/10.52907/jipit.2026.614

Posthumous Data Privacy in Kenya

*Timothy Samson Omondi Ayuo**

ABSTRACT

The digital age has redefined the boundaries of life, death, privacy, and ownership of personal information. Behind every dataset is a human being alive or postmortem private data with inherent dignity. While data privacy frameworks in Kenya, most notably the Data Protection Act, 2019, safeguard the rights of living natural persons, they remain silent on the status of personal data after the death of these living natural persons. This legal gap raises privacy, ethical, and legal questions on the control, inheritance, and value of digital assets and posthumous personal data. Consequently, sensitive health records, financial information, social media accounts, and digital correspondence remain vulnerable to misuse, exploitation, or erasure without consent from heirs or designated representatives. Unlike Kenya, the Republic of China and Rwanda acknowledge posthumous privacy and expressly recognize inheritance rights over personal data. This paper adopts a doctrinal legal research method and, guided by the dignity theory and autonomy theory, it argues for the necessity of legal recognition of posthumous privacy in compliance with constitutional rights to privacy and dignity. As evidenced by the exposure of health data in post-mortem reports following Gen-Z's 2024 finance bill protests, unregulated posthumous data can lead to identity theft, reputational harm, erosion of dignity and economic loss to beneficiaries. The author highlights international and regional practices on posthumous privacy. Lastly, the author recommends embedding posthumous data rights into Kenya's data protection regime, acknowledging that even in death, personal data continues to tell a tale of dignity, accountability, and legal recognition.

Keywords: Digital Remains, Legal Vacuum, Personal Data, Posthumous Data Privacy, Right to Erasure

* Ayuo Timothy Samson Omondi, LL. B (Moi University); PGDL; M.A. Governance & Ethics in view. ECPC-B DPO (Maastricht). Data Privacy Expert, PrivacyPulse Consulting Inc. (US); Researcher, Moi University. Tutored JKUAT & MKU universities. Email: timothyayuo@gmail.com

TABLE OF CONTENTS

ABSTRACT 15

I. INTRODUCTION 17

II. THE CONCEPTUAL AND PHILOSOPHICAL FOUNDATIONS OF POSTHUMOUS PRIVACY 21

A. Constitutional Lens and Background to the Problem 21
B. Autonomy Theory: Privacy as Self Determination 24
C. Dignity Theory: Privacy as Human Dignity and Personal Right 28
D. Opposition To Posthumous Privacy 32

III. POSTHUMOUS PRIVACY GAP IN KENYA 35

A. Posthumous Data Privacy Gaps in Complementary Laws 37

IV. COMPARATIVE JURISPRUDENCE 40

A. Insights from Rwanda 41
B. China's Approach to Posthumous Data 44

V. PROTECTING POSTHUMOUS DATA IN KENYA 47

VI. CONCLUSION 52

REFERENCES 55

I. INTRODUCTION

'O mortal vanity! How strange the age where man has woven his soul into the internet, and his memory into clouds unseen. In yester-years, the grave was the end of all whisperings the tongue silenced, the heart still. Yet now, though the body turns to dust, personal data lives on a spectral echo of the self, wandering the boundless ether with digital footprints. The dead, who in former times did rest in solemn peace, are summoned again, not by trumpet nor spirit, but by algorithm and code'.

-Anon.-

Kenya's Data Protection Act, 2019 (DPA) marks an important step forward in protecting the privacy rights of its citizens. That DPA legislation was timely and crucial cannot be belabored. Justice Jairus Ngaah's reasoning in *Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Ex parte); Immaculate Kasait, Data Commissioner (Interested Party) [2021] KEHC 122 (KLR)* supports this position. Under paragraphs 97-101, he interpreted the DPA as the statutory framework enacted to give effect to *Article 31 of the Constitution* by protecting the privacy of individuals and providing data subjects with rights and remedies in relation to the processing of personal data. The judgment, however, did not address whether protection extends to deceased persons, leaving the question of posthumous data privacy unresolved in Kenyan jurisprudence.

Further, as a testament to protecting privacy rights, the Data Privacy and Governance Society Report of 2025, for ODPC determinations, attests to that fact. The ODPC made 51 determinations in 2024. Complaints made to the ODPC in 2024 spanned sectors such as financial, health, education, and digital lending (DPGSK 2024 Report, p. 3). However, it contains a significant and damaging silence: it does not protect the personal data of individuals after they die. The DPA under section 2 defines a 'data subject' as a natural person, which means that the moment a person dies, their digital records, social media profiles, health

data, biometric information, emails, and cloud storage effectively fall outside the law's protection.

This research notes that there is currently no reported Kenyan case that has directly and squarely prosecuted or adjudicated a claim framed specifically as 'posthumous data privacy' of a deceased person under the Data Protection Act, 2019 or any other statute. Jurisprudence on privacy in Kenya has developed around natural living persons. This is a sentiment echoed by Ephraim Kenyanito and Sigi Mwanzia (The Star, 13 April 2021). The authors observe that: 'The Data Protection Act, 2019 only refers to (living) natural persons' and that Kenyan privacy and data protection rights are generally understood to cease upon death, leaving ownership and access to a deceased person's digital assets largely unresolved.

This is a problem in a country where digital footprints are increasingly permanent and wide-reaching. Corporations, data brokers, and even state agencies can repurpose a deceased person's data without consent, ethical limits, or legal accountability. Harbinja (2017) explains that once a person dies, many data protection regimes cease protecting that individual's personal data. Consequently, digital platforms and service providers often determine access, retention and disclosure through contractual terms rather than privacy law (Harbinja, 2017, pp. 66-88). The dead are left unguarded, their dignity vulnerable, and their digital memory open to misuse.

The problem extends beyond the deceased alone. Edina Harbinja (2022) posits that families and loved ones face real harm when a person's private data - health records, financial details, or personal communications - are exposed, distorted, or commercially exploited after their death. As Harbinja argues, the absence of post-mortem privacy protection leaves both the dead and their families vulnerable to reputational distortion, identity misuse, and emotional distress (Edina Harbinja, 2023).

There is also a growing economic dimension to this problem. Digital assets, ranging from influencers' social media accounts to artists' email archives and whistleblowers' encrypted files, carry real financial and reputational value (Naomi Cahn, 2019). Without clear legal rules on who owns or controls these assets after death, posthumous data becomes a site of confusion, dispute, and exploitation. As Kenya's digital economy in fintech, health-tech, and AI continues to expand, this legal vacuum threatens not only individual dignity but also broader consumer trust and digital ethics.

Kenya's constitutional commitment to human dignity under Article 28 and privacy under Article 31 provides a strong and sufficient basis for recognizing posthumous privacy rights; and the Data Protection Act, 2019 must be reformed to protect the personal data of deceased individuals, thereby bridging a legal gap that currently leaves the dead, their families, and Kenya's digital economy exposed to serious harm.

The paper advances four main arguments in support of its thesis. Firstly, dignity survives death. *Article 28 of the Constitution of Kenya (2010)* establishes human dignity as a foundational, justiciable constitutional value that informs the interpretation of all other rights. Because dignity is not extinguished by death, it provides a constitutional basis for protecting posthumous data privacy.

Secondly, the current legal gap causes real harm. The definition of 'data subject' as a natural person in the DPA creates a regulatory vacuum that enables data exploitation, reputational distortion, identity misuse, and emotional harm to families. In addition, the narrow interpretation of 'personal data' as espoused in *Allen Waiyaki Gichuhi & Charles Wamae v. Florence Mathenge & Ambrose Waigwa (2022) eKLR makes* it unclear as to how personal data should be interpreted. Posthumous data privacy violations also harm people before death by deterring autonomous living and causing anticipatory distress. The law cannot keep shying away from that harm.

Thirdly, some countries support reform. Jurisdictions, including EU member states empowered by GDPR Recital 27, the UK, Israel, Rwanda, and China, have begun extending privacy protections beyond death, recognizing posthumous data as an extension of human identity. Kenya's failure to do so leaves it behind in data privacy jurisprudence and exposes it to the regulatory gaps identified in cases such as *Webber v Information Commissioner and Cabinet Office [2017]* and *Trott & Skinner v Information Commissioner [2022].* Both persuasive cases confirmed that it would be an actionable breach of confidence for the relevant public authorities to disclose the deceased's hospital or care records to those who were not personal representatives, even if they could apply to become so or were next of kin.

Fourthly, reforms would align the law with Kenya's digital future. As Kenya's digital economy grows across fintech, healthtech, and AI, the question of who owns and controls posthumous digital assets, from a deceased influencer's social media accounts to an artist's email archives, is no longer theoretical. Without legal reform, posthumous data becomes a disputed inheritance vulnerable to misuse, litigation, and commercial exploitation. Incorporating posthumous privacy into the Data Protection Act, 2019 would align national law with constitutional values, global privacy standards, and the ethical expectations of Kenya's growing digital society.

To achieve the above aims, this paper employs a doctrinal and comparative legal research methodology. It examines Kenya's existing constitutional and statutory framework, places it within the broader philosophical tradition of human dignity and personality rights theory, and draws on comparative jurisprudence from Rwanda and China. This paper is structured in six parts. Part I, the introduction, exposes the legal gap under the Data Protection Act, 2019; Part II evidences the problem and grounds posthumous privacy in human dignity theory and personality rights; Part III dwells on the posthumous privacy vacuum in complementary laws; Part IV undertakes a comparative

jurisprudence from Rwanda and China; Part V is on policy reform recommendations; and Part VI offers conclusion and directions for future research.

II. THE CONCEPTUAL AND PHILOSOPHICAL FOUNDATIONS OF POSTHUMOUS PRIVACY

A. Constitutional Lens and Background to the Problem

The Constitution of Kenya, 2010 is built on a foundation of rights, values, and principles. Among fundamental rights are Article 28, which protects the right to human dignity, and Article 31, which protects the right to privacy. In reference, Prof. Yash Ghai and Jill Ghai (10 December 2018) observe that human rights are the spine of the Constitution. Chapter Four, the Bill of Rights, is the longest chapter, setting out both the norms of rights and the mechanisms for their fulfillment, though rights also appear across several other chapters (Ghai & Ghai, 2018, para. 3). The reasons given for recognizing these rights are to preserve the dignity of individuals and communities, promote social justice, and realize the potential of all human beings (Ghai & Ghai, 2018, para. 2).

In light of section 2 of the DPA 2019 and its accompanying Regulations, it is possible that these provisions were drafted with a life-centric view of privacy rights which exist only for living individuals, and end at death. This reflects a broader historical assumption captured in the old adage that '*dead men tell no tales*'. In addition, the limiting fact that the right to privacy is not absolute somewhat restricts a broader interpretation of privacy rights. This was emphasized by Lenaola J. at paragraph 22 in *JLN & 2 Others v. Director of Children Services & 4 Others [2014] eKLR.* In that case, the issue was whether the hospital's disclosure of the petitioner's medical records to a third party violated the petitioner's right to privacy guaranteed under Article 31 of the Constitution of Kenya, 2010. It was held that the Hospital did not violate the petitioners' right to privacy when it

divulged information about the surrogacy agreement while seeking the advice of the Director on what to do about the circumstances involving the petitioners and the Hospital. The Director, however, violated the petitioners' rights and fundamental freedoms, including their right to dignity, by seizing the children and placing them in a children's home.

A person's digital life continues long after death, spread across social media platforms, cloud servers, health databases, financial records, and biometric systems. This creates what is loosely called a '*digital afterlife*,' a persistent online presence that continues to circulate, influence, and even generate income for others, while remaining entirely beyond the control of the person whose identity it represents (Dr. Shaji and Mamedova, 2024, pp. 4-5).

Internationally, jurisdictions such as Rwanda and China, as discussed in subsequent chapters in this paper, have policies to grapple with post-mortem data protection, recognizing that posthumous privacy is necessary for human dignity. In the EU context, Recital 27 of the GDPR allows member states to make their own rules on post-mortem data, acknowledging the gap even at the supranational level.

Notably, some court decisions from comparable legal systems shed light on the issue. In *Ajemian v. Yahoo! Inc.* (Massachusetts Supreme Court, 2017), John Ajemian died intestate in 2006, and his siblings were appointed as the personal representatives of his estate. The estate administrators requested access to his Yahoo email account to identify estate assets and notify contacts. Yahoo! denied the request, arguing that the federal Stored Communications Act (SCA) prohibited voluntary disclosure of emails and that its Terms of Service (TOS) gave the company discretion to deny access to deceased users' accounts. The court ruled that federal law does not bar email providers from giving a decedent's personal representatives access to their emails, and that personal representatives can provide lawful consent to release those records.

The Massachusetts Supreme Court held that the SCA does *not* prohibit an email service provider from voluntarily disclosing a decedent›s email contents to the personal representative of their estate. Personal representatives legally qualify as 'agents' of the user and can provide 'lawful consent' for the release of the emails. The court set aside the summary judgment that favored Yahoo!, as there were genuine issues of material fact regarding the enforceability of Yahoo!'s TOS.

In a persuasive matter on privacy, the UK Upper Tribunal (Administrative Appeals Chamber) pronounced itself on the importance of safeguarding posthumous health data. In *Webber v Information Commissioner and Cabinet Office [2017] UKUT 312*, the court confirmed that disclosing deceased persons' hospital or care records to those without proper authority could amount to a breach of confidence, a recognition that the dead retain some residual privacy interests. The Kenyan case of *MWK & Another v Attorney General & 4 Others [2017] KEHC 1496* is equally instructive: the High Court held that dignity is a foundational constitutional value that informs the interpretation of all other rights, including privacy, and that any infringement must survive the Article 24 limitation test.

Therefore, this chapter examines and reviews literature from philosophical concepts that birthed the importance of dignity and privacy in life, and beyond life to after death, which by extension informed the need for posthumous data privacy. Accordingly, this paper uses the *Autonomy theory* and *the Dignity theory* as the backbone of the push for posthumous privacy, borrowing from the opinions of scholars and philosophers. Privacy is at the core of the concept of dignity. It is unequivocal that autonomy and dignity are the threads that run across posthumous data privacy and are discussed in depth hereunder as the autonomy theory and the dignity theory.

B. Autonomy Theory: Privacy as Self Determination

Scholars' views abound on this theory. The *Autonomy Theory*, advanced by Alan F. Westin (1967), views privacy as an expression of personal self-determination. It frames privacy not merely as secrecy but as the individual's authority to decide when, how, and to what extent personal information is shared. Privacy protects the individual's capacity to shape their life narrative, exercise meaningful consent, and maintain control over their identity. Westin's (1967) account remains foundational in contemporary data protection frameworks, especially those emphasizing informational self-determination as a core component of human dignity.

Privacy as personal autonomy places informational control at the core of individual freedom, arguing that people must be able to determine when, how, and to what extent information about them is shared (Westin, A. F., 1967). This understanding is consistent with John Stuart Mill's (1859/1978) liberal harm principle, which holds that individual liberty may only be restricted to prevent harm to others, implying that unwarranted intrusion into personal data constitutes a form of harm that undermines self-governance. Westin's theory also aligns with Immanuel Kant's (1785/1996) conception of dignity, where each person is treated as an end in themselves rather than a means to institutional, commercial, or state objectives. By grounding privacy in autonomy, harm prevention, and respect for human dignity, these liberal philosophies collectively support a robust normative foundation for both contemporary and posthumous data protection.

McCallig (2014) argues that modern justifications for privacy, particularly autonomy and dignity, do not vanish upon death but remain relevant to how a person's data and memory are treated. He suggests that protecting posthumous privacy affirms societal respect for personhood, even after physical demise.

Daniel J. Solove (2008) argues that privacy is not a single concept but a cluster of related problems arising from different types of harmful information flows. He critiques reductionist interpretations that limit privacy to control or access and instead develops a taxonomy identifying four main categories of privacy problems: information collection, information processing, information dissemination, and invasion. Solove's taxonomy reflects a shift from an abstract moral right to a pragmatic framework for regulating harm. In his view, privacy violations arise not merely from disclosure but from the process and power dynamics behind data management. This approach is invaluable in contextualizing posthumous data privacy in Kenya, where the dead remain vulnerable to reputational damage, identity misuse, and unauthorized data monetization.

Gloria González Fuster (2014) situates privacy within the human rights discourse, grounding it in the principle of human dignity. Fuster (2014) argues that privacy and data protection are expressions of human dignity, autonomy, and identity. For Fuster, privacy is not merely about individual choice but about societal recognition of personhood. Her argument reflects a philosophical shift: privacy serves as a safeguard for human dignity against commodification and surveillance. This aligns with the moral necessity of protecting personal data even after death since data continues to represent the person's identity, relationships, and legacy. Fuster's perspective emphasizes that data protection extends beyond economic concerns to the ethical recognition of individuals as moral beings deserving of respect, even in the digital afterlife.

The Autonomy theory of privacy similarly reinforces posthumous privacy claims. Rooted in liberal philosophy, including Mill's harm principle and Kant's conception of dignity, autonomy-based privacy understands personal data control as essential to self-determination. Modern legal expressions of this theory, from *Germany's Census Case (1983) BVerfGE 65, 1-Census Case (Volkszählungsurteil),* Federal Constitutional Court of Germa-

ny, established the principle of 'informational self-determination', holding that individuals possess the right to control the disclosure and use of their personal information. The judgment recognized personal data as closely linked to individual identity, dignity, and self-determination.

Alan Westin's foundational account of privacy as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others presupposes a subject capable of exercising that claim (Westin, 1967). The moment of death removes that subject. What remains is not autonomy, but its residue: intentions expressed during life, relationships formed, narratives constructed, and the question the law must answer is whether any of that residue generates enforceable informational entitlements that survive the person who created them.

Beate Rössler's analysis offers the most useful bridge. She argues that autonomy, in the privacy context, is not merely about present control but about the conditions under which a person was able to construct and project a coherent self during their lifetime (Rössler, 2005). On this account, posthumous exposure of information that the deceased withheld or would have withheld during life is not a neutral act after the fact; it retroactively disrupts the autonomy the person actually exercised while alive. It changes, without consent, the terms on which they presented themselves to the world. The deceased cannot object. But that incapacity is precisely the problem, not the answer.

Janna van der Linden-Koot, building on James Rachels' claim that privacy enables different kinds of relationships by allowing selective disclosure, argues that posthumous disclosure collapses those carefully maintained distinctions permanently and irreversibly (Rachels, 1975). A person who confided their HIV status to a doctor but not to their employer, or their religious doubts to a friend but not to their congregation, exercised autonomy through that selective disclosure. Posthumous revelation of either secret does not merely breach a current preference;

it undoes a deliberate act of self-governance that shaped how that person lived and related to others. The harm is retrospective, but it is a harm to a real exercise of autonomy, not a hypothetical one.

This is where proxy autonomy becomes analytically plausible. If autonomy in the privacy sense includes the capacity to structure one's informational environment during life, then it is not incoherent to argue that proxies - heirs, executors, or designated representatives - can enforce those structures after death, not because the deceased retains autonomous agency, but because giving legal effect to pre-mortem informational choices is the only means of preserving the genuine autonomy that was exercised while the person lived. Edward Bloustein (1994) captured something close to this when he argued that privacy protects the integrity of the individual personality - an integrity that does not vanish because the person has. Proxy enforcement is not a fiction of continued agency; it is the law's recognition that autonomy, to mean anything, must be capable of outlasting the moment it was exercised.

Similarly, the decision in K.S. Puttaswamy v. Union of India (2017) is a landmark Indian Supreme Court decision that constitutionally recognized the right to privacy as a fundamental right under the Indian Constitution. The Court emphasized that privacy includes decisional autonomy, informational control, and the freedom to determine how personal data is collected, used, and shared.

In the EU, *the Schrems I* and *Schrems II* decisions exemplify the autonomy theory of privacy.

In *Maximillian Schrems v Data Protection Commissioner (Case C-362/14), CJEU (2015) (Schrems I)*, the Court of Justice of the European Union implicitly affirmed this view by holding that indiscriminate access by foreign intelligence services strips individuals of meaningful control over their data. The invalidation of the Safe Harbour framework thus became a defense of

personal autonomy: without constraints on surveillance, Europeans cannot exercise agency over how their digital footprints are used or interpreted (Hollis, D. et. al, 2022). This therefore limits their autonomy over their privacy.

The decision in *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18), ECLI:EU:C:2020:559 (Schrems II)* amplified this logic. The Court's concern with disproportionate surveillance and inadequate redress mechanisms reflects a commitment to protecting informational autonomy. When individuals lack the capacity to challenge or even understand how their data is processed, their ability to make autonomous life choices is undermined. The decision's emphasis on 'essential equivalence' between EU and third-country protections signals that autonomy cannot be compromised merely because data crosses borders (Zimmer, V., 2021).

C. Dignity Theory: Privacy as Human Dignity and Personal Right

This paper maintains that the starting premise is that personal information is not merely a collection of neutral facts but can constitute an enduring representation of an individual's personality, identity, relationships, and dignity. Continued retention and disclosure after death may therefore affect how the deceased is represented and understood, as well as surviving relatives and the integrity of historical records. Personal data embodies aspects of personality and identity. This representation may persist after death, and continued disclosure can impact personality, dignity, and the interests of survivors. Consequently, certain legal protections may justifiably extend beyond an individual's death. That ushers in the dignity argument.

Dignity theory of posthumous privacy pursues a logical chain. Bloustein (1964) premised that privacy safeguards personhood itself, not merely secrets, meaning dignitary harm survives the person. Rupniewski (2020) extended this, arguing that

dignity is a normative status grounded in rational agency, not biology, and therefore persists after death. Harbinja (2017) distinguished between exercising rights and holding the interests those rights protect, the latter surviving death because they are social, not subjective. Dworkin (1993) clinched the argument: critical interests, including informational self-determination, retain moral weight posthumously. Together, these premises build an irrefutable case for posthumous data law reform. Charles Fried (1970) premised that privacy is not merely instrumental but constitutive; without it, love, friendship, and respect are structurally impossible, because those relationships depend on selective informational sharing. Privacy therefore creates the relational architecture of a dignified human life. Małagocka (2018) built on this, arguing that personal data is an extension of identity itself; data about a person is not separate from that person but is part of how they exist socially. Violation of data privacy is therefore violation of the person. Čtvrtik (2021) reasoned that because data constitutes identity relationally, posthumous data exposure reconstructs the person without consent, making posthumous protection a dignity imperative.

The above scholars' conclusions on the dignity theory are highlighted as follows. A major proponent of the 'Dignity Theory' supporting privacy as a human dignity and personality right is Edward J. Bloustein (1984/2009), who argued that privacy is closely tied to human dignity and the integrity of personality. Bloustein (1984/2009) makes the normative argument that privacy protects the moral and psychological core of the person.

Bloustein's dignity-grounded theory of privacy emphasizes that informational control is not merely a matter of convenience, but a safeguard for the moral and psychological integrity of the individual (Bloustein, 1984/2009). Contemporary scholars build on this foundation: Rupniewski (2023) reconnects dignity to a robust personalist legal framework, arguing that the law should treat every human as a person with inalienable worth, deserving consistent respect and protection. Building on the premise, Čt-

vrtnik (2023) applies this framework to archives and post-mortem data, contending that personality rights and dignity should survive death and govern the handling of digital remains.

Closely related is the *dignity theory*, which treats privacy as an essential component of human worth. Civil law traditions, especially in Germany and France, ground privacy in the general personality right, an expression of the intrinsic value of the human being. The EU Charter's separation of privacy and data protection (Articles 7 and 8) reinforces this moral framework. Dignity-based privacy is less about secrecy and more about recognition, respect, and treating individuals as moral agents. Charles Fried similarly describes privacy as the security of control over personal information, underscoring the seriousness of that right (Fried, p. 493). If dignity endures beyond death, as many philosophers contend, posthumous data must be handled with the same respect accorded to living persons.

Ronald Dworkin's (2011) account of life-transcending integrity offers a compelling starting point. In his later work, especially Justice for Hedgehogs (2011), Dworkin argues that living well requires integrity: a person must strive to make their life a coherent story in which their choices and values align in a unified narrative. This narrative, however, does not conclude at biological death. Dworkin maintains that individuals have an enduring interest in how their lives are interpreted, remembered, or judged after they die. Posthumous events such as exposure of private data, reputational harm, or distortion of one's beliefs can undermine the dignity and coherence of that life narrative. Protecting posthumous privacy thus becomes a moral duty, preserving the unity and meaning of a person's life even after death.

Harbinja et al. (2024) argue that service users expect dignity-preserving choices for their digital remains and call for legal and platform reforms to reflect those expectations. Harbinja's work underscores a persistent gap between what users expect for the posthumous handling of data and current legal and commercial practice, a gap she frames in terms of dignity and autonomy.

Additionally, Nwabueze (2024) argues that dignity and memorial interests justify rethinking legal silence on post-mortem privacy in England and Wales. They are unjustifiably silent on post-mortem privacy despite strong conceptual foundations for protecting the deceased. He contends that human dignity does not expire at death; rather, it persists through the moral weight of one's reputation, identity, and the respectful treatment of personal information. Nwabueze further introduces the idea of memorial interests: the living's legitimate concern in how a deceased person is remembered, especially close family members. These intertwined *dignity* and *memorial interests*, he argues, create a compelling justification for revisiting the absence of statutory or common-law protection for posthumous privacy.

Health data is also a sensitive area for posthumous privacy, and a scholar, Małagocka (2024), situates dignity as a corrective to emergent 'digital unfreedom', recommending regulatory frameworks that preserve autonomy and dignity in health-sensitive contexts. Małagocka argues that the rapid expansion of digital technologies, especially in health-sensitive environments, has created conditions of 'digital unfreedom', where individuals lose meaningful control over how their intimate data are used. She situates human dignity as a central corrective to these emerging risks, asserting that dignity requires protection not only against exploitation but also against subtle forms of informational domination. Małagocka recommends regulatory frameworks that reinforce personal autonomy, ensure transparent data practices, and embed dignity as a guiding value in health-data governance. Her analysis positions dignity as both a moral anchor and a practical safeguard in contemporary digital regulation.

The dignity theory also underscores that data protection expresses society's respect for personhood, which does not vanish at death. The High Court in *MWK & Another v Attorney General & 4 Others Con. Pet. 347 of 2015 [2017] HC 1496KL* clearly explained the court's position on upholding human dignity. In this case, a strip search of a minor by the police was deemed

unconstitutional and publication of photos amounted to serious invasions of privacy and dignity. The judge held that dignity is a foundational right whose infringement must be justified under the strict limitation test provided for under Article 24 of the Constitution of Kenya.

Taken together, these philosophical and legal insights reveal that posthumous privacy is not merely an abstract ideal but a necessary extension of dignity, autonomy, and integrity.

D. Opposition To Posthumous Privacy

Academic opinions and challenges abound about protecting privacy after death. Some argue that privacy is conceptually tied to the autonomy and interests of a living rights-holder and therefore cannot meaningfully survive death. Wacks (2013) maintains that privacy is inseparable from individual agency and self-determination, both of which extinguish upon death; consequently, the deceased cannot be bearers of privacy rights. This view is grounded in the broader interests-based theory of rights advanced by H. L. A. Hart, who argued that rights exist to protect the interests of living persons and therefore cannot subsist once those interests cease (Hart 1982). Westen (1982) similarly rejects the notion of rights without persons, contending that legal rights presuppose a subject who can exercise or benefit from them, which makes posthumous privacy logically incoherent.

Rosen (2000) expresses similar concerns, arguing that binding the living to the privacy expectations of the dead may hinder access to truth, public-interest journalism and historical inquiry. In the archival field, Ketelaar (2002) cautions that strong posthumous privacy restrictions can impede the preservation and accessibility of archival records, thereby limiting society's ability to reconstruct and understand its past.

A strong case is made that the harm of posthumous privacy violations is not confined to the dead. Scarre (2012) contends that '*we feel strong distaste while alive for the prospect of our loss*

of privacy when dead' (p. 10). Building on this, Davey T. (2020) identifies three concrete ways posthumous privacy failures harm the living: first, by frustrating a person's critical interest in maintaining a private life that extends beyond death; second, by causing people to change or inhibit their behavior in life out of fear that their actions may become public after they die; and third, by causing actual distress during a person's lifetime when they harbor secrets that they fear will be exposed upon their death. These insights demonstrate that posthumous privacy protection is not merely symbolic: it has real, present-tense consequences for how people live.

Some common-law courts support this narrow view. In Deepa Jayakumar v. A.L. Vijay (2021), the Madras High Court (Division Bench- R. Subbiah & S.K.S. Kurup, JJ) decision of 16 April 2021, the court held that the right to privacy of an individual:

> 'Inheres in the human being by birth…remains with the human being till he/she breathes last. … It is born with the human being and extinguishes with the human being.' The court further held: 'A privacy or reputation earned by a person during his or her lifetime, extinguishes with his or her death. After the death of a person, the reputation earned cannot be inherited like a movable or immovable property by his or her legal heirs.'

These views, however, focus on legal enforceability rather than moral continuity. Philosophers like Charles Fried and contemporary scholars such as Gloria González Fuster highlight that dignity is not reducible to enforceable claims but reflects society's valuation of the human person (Fuster, 2014). This moral foundation supports extending privacy protection even where statutory law is silent.

Legal-economic perspectives also question whether posthumous privacy serves any meaningful function. Posner (1981) argues that privacy is instrumental and primarily valued for the advantages it confers on living individuals; once a person dies and is no longer capable of experiencing harm or benefit, the rationale for privacy protection evaporates. Earlier economic theorists, such as Fried, have similarly suggested that privacy oper-

ates within a framework of incentives and welfare for the living, a rationale that loses force after death.

Still on the opposing views, the idea of linking privacy, autonomy, and trust was robustly contested by Hongladarom (2016), who claimed that in a close-knit society, individuals know very well the small details about each other and trust one another. So, in this society, trust becomes the cornerstone for developing the society, even though there is no privacy and it becomes unnecessary for autonomy to function. Once the individual can make a decision of his own will, he has autonomy even though his details are known by others. Yet, he confirmed the relationship between privacy and accountability, pointing out that:

> *'The need for privacy protection then becomes almost universal. Furthermore, if one is not accountable for what one does, then there would be no means to sanction anyone's behavior, including snooping and violating others' private personal space. So, if there is no accountability, it is very likely that there is no privacy either' (*Hongladarom, 2016).

Thus, this view advocates that the best way to understand concepts of privacy, autonomy, trust, and accountability is to conceive of them as distinct rather than define them in relation to one another. Collectively, these scholars argue that posthumous privacy either lacks a conceptual foundation or imposes unjustifiable costs on societal interests. Their critiques highlight the tension between respecting the dignity of the deceased and facilitating transparency, historical truth, and public access to information. Finally, the concept of 'privacy' does not seem to have a uniform definition and is not accorded straightforward legal treatment. Unfortunately, this author believes that these opposing views are generally weak.

Firstly, on the point that privacy ends with individual agency after death: human dignity and reputational interests often survive death, and that is the concern even for heirs of the deceased. Agency can be exercised by proxy, hence provisions of next of kin. Legal systems already protect estates, reputation, and burial rights posthumously, showing some personal inter-

ests continue beyond death, such as dignity and the right to privacy.

Secondly, on the point that dead persons cannot exercise rights: numerous legal rights survive death through representatives, including copyright, succession, and defamation-related interests. Posthumous privacy can equally be exercised through estates or designated beneficiaries by the deceased who dies testate.

Thirdly, on the point that privacy rights are purely personal and non-transferable: digital data affects surviving family members, reputational legacy, and societal dignity interests. Posthumous privacy therefore extends beyond individual control into relational and societal protection concerns on the death of a data subject.

Fourthly, on the point that privacy laws are utilitarian and only benefit the living: protecting posthumous data encourages trust in digital systems during life, assuring individuals that their dignity, communications, and personal information remain respected after death, thereby enhancing freedom to express themselves when alive. Arguably, fear of negative repercussions posthumously to the deceased's family would to an extent limit their freedom.

Lastly, on the point that dead persons suffer no harm, while true for the dead, posthumous misuse of data can damage family dignity, historical truth, reputation, and cultural memory, creating tangible social and emotional harms despite the subject's death.

III. POSTHUMOUS PRIVACY GAP IN KENYA

Kenya was the first country in East Africa to enact a data protection law in 2019. It pioneered privacy laws, but laws are living documents that thrive on amendments, and there is no perfect document. Societal changes such as the advent of tech-

nology demand changes in law that keep pace. Of note, the DPA's definition of 'data subject' covers identifiable natural persons. Further, it defines a data subject under *section 2* as '*an identified or identifiable natural person who is the subject of personal data*'. Garner B. (2019) Black's Law Dictionary defines a natural person as a human being, as distinguished from an artificial person created by law. It is therefore evident that the DPA, 2019 is designed to protect the rights and privacy of living individuals concerning their personal data. When an individual dies, the legal landscape becomes nuanced. This paper argues that the statute explicitly contemplates only living persons, thus raising the question of whether rights survive death. It submits that it is indeed factual that under the DPA's provisions, data privacy ends with the death of a living data subject.

Further, *Section 26* of the DPA, 2019 provides for data subjects' rights, including the right to access, rectification, objection, and deletion of their data, all framed in the present tense and premised on an existing legal personality capable of exercising them. Under this framing, death extinguishes legal personality under Kenyan law, meaning a deceased person cannot exercise, waive, or enforce these rights. The DPA's enforcement mechanism reinforces this reading. Complaints to the Office of the Data Protection Commissioner (ODPC) pursuant to *section 56* require an aggrieved data subject to lodge the complaint, something a deceased person is legally incapable of doing. Under the introduction section in this paper, the narrow definition of personal data is highlighted. Still on the concept of personal data, a German court also elaborated on the meaning of 'personal data' in *Patrick Breyer v Bundesrepublik Deutschland, Case C582/14, Judgment of the Court (Second Chamber), 19 October 2016, ECLI:EU:C:2016:779.* At paragraph 32, according to Tosoni, L. et al. (2020):

> 'Personal data' means *any information relating to an identified or identifiable natural person ('data subject').* Pursuant to that provision*, an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification*

number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.' [emphasis added]

Therefore, the EU GDPR definition is broad in concept compared to the DPA, 2019. Such a narrow definition in the DPA, 2019 only breeds room for unclear interpretation, which is a problem. Notably, there is a grave absence of posthumous privacy cases; the only case this paper assessed, inclined towards posthumous data privacy in Kenya, is *Mwaniki v Attorney General [2023] KEHC 22385 (eKLR)*. In their decision, the court observed that privacy matters, even in death, and ruled that the petition before it was unmerited and was thus dismissed, citing lack of locus standi. The Petitioner had not obtained letters of administration, a legal prerequisite to acting on behalf of a deceased estate, and the court held that releasing the requested information of the deceased's sensitive financial data to the petitioner, who was the son of the deceased, would amount to an unlawful invasion of privacy, a breach of professional confidentiality, and an impediment to due process under *the Law of Succession Act (Cap 160).*

This paper highlights other complementary laws in Kenya to the DPA, 2019 that handle posthumous data, especially health data. However, they also fall short in terms of adequately protecting posthumous privacy. This paper, in a nutshell, briefly highlights some shortcomings in the complementary laws.

A. Posthumous Data Privacy Gaps in Complementary Laws

Apart from the DPA, 2019, Kenyan legislation offers only fragmented and indirect protection for the personal information of deceased persons. Several statutes regulate administrative or medical processes surrounding death, yet none articulate a coherent right to posthumous informational privacy. This paper submits that the provisions provided are not exhaustive but merely guiding. *The Births and Deaths Registration Act, Cap 149*, under sections 2, 7 and 15, requires registration and storage

of death records that contain identifiable personal data such as names, dates, causes of death, and familial details (Births and Deaths Registration Act, Cap. 149). These records were historically intended for administrative certainty, not privacy protection, and the Act is silent on confidentiality, data retention, or limits on downstream use. In an era where cause-of-death data may reveal sensitive medical conditions, this statutory silence exposes deceased persons and their families to potential misuse of intimate information.

Similarly, there are *the Public Health Act Cap. 242* under sections 36(a), 69, 144 and 148 on the speedy interment of the dead; and *the Public Health (Public Mortuaries) Rules, 1991* on the publication and description of unclaimed bodies in local newspapers including revealing health data. They regulate the handling, storage, and disposal of bodies but do not address the handling of mortuary records, which often include photographs, medical notes, post-mortem findings and other forms of sensitive personal data (*Public Health Act, Cap. 242*). The law focuses on sanitary and administrative concerns, but imposes no clear duties on mortuary officers or hospitals to safeguard the confidentiality of such information or to limit disclosure to third parties, including media organizations or commercial actors, alive to the fact that a public health issue can be an exception to health data privacy as witnessed during the COVID-19 pandemic.

A further gap emerges in the context of medical teaching and research under *the Anatomy Act, Cap 249* in sections 6, 7, 10, 11, 12, 13, 14, 15 and 16. Although the Act establishes procedures for the donation and use of bodies for anatomical examination, it is premised almost exclusively on the physical handling of human remains. It does not address the confidentiality of donor data, the anonymization of identities, restrictions on the circulation of photographs or imaging records, or controls over digital datasets generated from cadaveric study. As a result, personal information linked to deceased donors may be accessed, retained, or reproduced without any statutory privacy safeguards.

The Kenyan *Penal Code (Cap.63)* is not robust in combating breaches of posthumous data privacy, as it fails to criminalize acts involving the misuse, exposure, or commercial exploitation of a deceased person's personal data that is in the form of digital print. It focuses narrowly on physical offenses against the dead, such as interference with a corpse, but leaves digital remains, medical records, images, and biometric identifiers unprotected. This legal silence enables media houses, data brokers, and even state agencies to disclose or process a deceased person's data without accountability. Without explicit penal sanctions, deterrence is weak, allowing harmful narratives, stigma, and unauthorized data circulation to flourish after death.

The Computer Misuse and Cybercrimes Act 2018 is the closest measure to safeguarding digital posthumous privacy, with provisions aimed at securing personal data such as section 14 on unauthorized access, section 19 on unauthorized disclosure of passwords or access codes to third parties, and sections 25 and 26 on computer forgery and fraud. Worth noting is that this legislation has been bedeviled with petitions challenging its provisions' constitutionality, following the 2025 amendments.

Across these statutes, the absence of a recognized posthumous right to informational privacy is the common thread. Kenyan law presumes that privacy interests extinguish at death, leaving families with limited standing to object to the circulation of sensitive medical, biographical or digital information about a deceased relative, unauthorized disclosure and exploitation, loss of informational self-determination, digital identity and impersonation, reputational and dignity harms and commercial exploitation among others. With no statutory framework governing digital remains such as social media accounts, biometric identifiers, photographs, or cloud-stored correspondence, technology platforms and private actors retain wide discretion over how a deceased person's data is handled. This regulatory vacuum is particularly acute where deceased individuals leave extensive digital footprints that may be misused, exploited, or publicly ex-

posed.

Collectively, these gaps illustrate that Kenyan law treats death primarily as an administrative or public-health issue, with little regard for the informational interests that survive death. The absence of clear duties of confidentiality and the lack of remedies for families contribute to a landscape in which posthumous dignity and privacy remain insufficiently protected. The subsequent discussion on comparative jurisprudence is an eye-opener for law reformers on jurisdictions already embracing posthumous data privacy in practice.

IV. COMPARATIVE JURISPRUDENCE

This comparative jurisprudence chapter traces how Rwanda and China's legal systems have made strides to recognize that personal data does not lose all moral or social value at death. Across some jurisdictions, posthumous data privacy has gradually moved from a neglected idea to an emerging principle of digital dignity. Countries such as Rwanda and China have introduced forward-looking protections that require continued respect for a person's posthumous information long after they are gone. For instance, China's *Personal Information Protection Law, 2021* recognizes the rights of close relatives to safeguard the data of deceased persons, while the European Union's General Data Protection Regulation, though centered on living persons, has inspired member states like Germany to adopt domestic provisions that extend privacy thinking beyond life.

Taken together, these developments show a developing trend towards acknowledging that identity persists in digital form and that it deserves measured legal protection. This offers Kenya a valuable reservoir of ideas. As Kenya's digital landscape expands and more personal information is stored, shared, and monetized, lawmakers can carefully study these developments to craft a framework that preserves dignity, guides data controllers, and offers clarity to families. Kenya can build a modern and

culturally grounded approach to posthumous data privacy that reflects its constitutional values and responds to the realities of a data-driven society.

A. Insights from Rwanda

Rwanda provides a legal framework that recognizes personal data interests beyond death. Under Law No. 058/2021 of 13 October 2021 on the Protection of Personal Data and Privacy, the law expressly applies to natural persons, which ensures that data protection does not end at the moment of death. Article 25 of Law No. 058/2021 specifically allows the designation of heirs to manage posthumous data. Aissatou Sylla (2021) notes that the statute allows individuals to designate an heir who may exercise certain rights over their personal data after they die. Although personal data itself is not subject to succession in the traditional sense, a designated heir may hold full or limited authority over how the deceased's data is processed, depending on what the individual instructed before death. This model preserves autonomy and dignity by allowing people to control the posthumous handling of their personal information and by providing a legally recognized representative to safeguard those interests.

Rwanda serves as a particularly relevant regional comparator for examining posthumous data privacy in Kenya, despite the significant limitation that its statutory framework primarily addresses the testamentary wishes of the deceased. The significance of Rwanda's approach is not to suggest that Kenya should adopt its legislation in its entirety, but rather to illustrate that an African legal system within a similar regional and constitutional context has already addressed a question that remains largely unresolved in Kenyan law.

Kenya's DPA, 2019 defines a data subject as an identified or identifiable natural person and structures substantive rights accordingly. Sections 26 and 27 provide rights of access, objection, correction, and deletion, and explicitly allow representation for minors, persons with disabilities, and individuals authorized by the data subject. However, the DPA does not establish a comparable statutory framework for deceased individuals. This legislative gap is precisely the issue that Rwanda's experience helps to clarify.

Key learnings from Rwanda are as follows. Firstly, Rwanda is an African comparator rather than a solely European reference. Rwanda is preferable to exclusive reliance on European jurisprudence because it provides a regional African response to a problem that arises within a similar legal, technological, and institutional context. Comparative law is most effective when it highlights a transferable legal issue rather than simply replicating a foreign solution. Rwanda's *Law No 058/2021 on the Protection of Personal Data and Privacy* directly addresses this issue through Article 25**.** This provision states that personal data is not subject to succession but allows a data subject who has left a will to grant full or restricted rights regarding data processing to an heir if the data remains in use. This is significant for Kenya because current Kenyan law provides minimal guidance regarding the disposition of personal data after death. Secondly, the testamentary limitation of the Rwanda approach is both a weakness and an analytical advantage. A primary criticism of Rwanda's model is justified: Article 25 of Law No. 058/2021 relies heavily on the existence of a will. As a result, it does not necessarily protect intestate deceased persons and does not establish a comprehensive, autonomous posthumous privacy right for all deceased individuals. This limitation should not disqualify Rwanda as a comparator. Instead, it offers a valuable critical lesson for the reform of Kenyan law. Kenya might consider several questions: *What should occur when the deceased has left no will? Who should be empowered to exercise data rights? How should conflicts between the deceased's instructions and the interests of*

surviving relatives be resolved? What standards should govern the treatment of medical, genetic, biometric, or family data?

Therefore, Rwanda provides an initial legislative model rather than a complete solution for Kenya. Thirdly, Rwanda illustrates that posthumous data protection does not require treating personal data as inheritable property. A notable aspect of Article 25 of Law No. 058/2021 is its clear conceptual distinction between personal data and inheritable property. Rwanda explicitly states that personal data is not subject to succession, yet allows individuals to designate rights regarding its processing through testamentary instructions. This distinction holds significant relevance for Kenya. Legal reform in Kenya should avoid categorizing personal data as an ordinary asset that can be inherited like land, shares, or money. Instead, the law could acknowledge ongoing privacy, dignity, and informational interests, while permitting an authorized individual to exercise specifically defined rights following the data subject's death. This approach aligns with scholarly arguments that post-mortem privacy necessitates a conceptual framework distinct from traditional property-based inheritance. Asta Tūbaitė-Stalauskienė (2018) observes that post-mortem privacy presents significant challenges because existing data-protection frameworks predominantly concern living persons, while digitally preserved information may continue to exist after death. Fourth, Rwanda offers a valuable connection between privacy and succession law. This aspect represents Rwanda's most significant relevance for Kenya. The issue is inherently interdisciplinary, as posthumous data intersects with privacy, succession, family relationships, health confidentiality, intellectual property, constitutional dignity, and digital inheritance. Rwanda's explicit inclusion of this issue within data-protection legislation demonstrates that it should not be addressed solely through succession law. Kenya could adopt a similar approach by developing a framework under the DPA, coordinated with the *Law of Succession Act*, health records legislation, and other relevant legal regimes. Fifth, Rwanda reinforces the rationale for legislative reform in Kenya. The comparative lesson is

not that Kenya should replicate Article 25 of Law No. 058/2021. Instead, Rwanda demonstrates that legislative recognition of posthumous data interests is feasible within an African jurisdiction. Lastly, giving the ODPC clear jurisdiction over posthumous-data complaints.

The case for using Rwanda as a comparator is most compelling when viewed as an exercise in comparative learning rather than direct legislative transplantation. Rwanda's significance lies in demonstrating that the posthumous data issue can be explicitly addressed in statute while maintaining the distinction between personal data and inheritable property. The limitations of Rwanda's testamentary approach also present Kenya with an opportunity to develop a more comprehensive legal model.

B. China's Approach to Posthumous Data

China's *Personal Information Protection Law (PIPL)* provides Kenya with a guiding model for addressing a legal gap in the DPA, 2019. Under Article 49 of the PIPL, close relatives of a deceased person may, for their own lawful and legitimate interests, exercise rights including consultation, copying, correction, and deletion of the deceased's personal information, unless the deceased made different arrangements before death. China therefore offers Kenya a practical legislative reference point. Kenya could amend sections 26 and 27 of its DPA, 2019 to specify which rights survive death and permit their exercise by appropriately defined representatives or close relatives, subject to legitimate interests and the deceased's wishes. Amendments are discussed subsequently in the recommendations section of this paper.

Not only that, but China also offers one of the clearest examples in Asia of a legal system that extends privacy and personality protections beyond death. Under the PIPL, 2021, personal data must be deleted once the purpose for which it was collected has been fulfilled, the service has ended, or the retention period

has expired. This framework allows an individual's data rights to continue after death, with deletion obligations and other safeguards effectively followed through by family members or representatives. Although rights are still evolving, the law indicates that personal information does not lose its legal significance upon a person's death. Relatives therefore act as legal representatives of the deceased's informational interests, especially where personal data affects family dignity, inheritance matters, reputation, or memorial interests. Notably, this is a departure from the Rwanda law that expressly deals with testate cases but encompasses both testate and intestate cases in posthumous data privacy. Matters in point manifest in certain cases.

In the case of *Guo X and Others v Shanghai XX Technology Company and Others* Beijing Internet Court, 2023 (Personal Information Protection Dispute), relatives of deceased platform worker, Li X, sued several technology companies after his work-platform account was deactivated following his death, preventing access to attendance and personal data relevant to investigating his death. The court held that close relatives could invoke rights under Article 49 of the Personal Information Protection Law to protect and access the deceased's personal information for legitimate interests, although direct account login was denied to protect third-party privacy.

Similarly, in *Kathy Chow Medical Privacy Incident (2023) Beijing*, administrative and criminal investigations arose from the unlawful disclosure of deceased actress Kathy Chow's medical records in Beijing. Following Kathy Chow's death, hospital personnel unlawfully disseminated her confidential medical information online. Chinese authorities initiated investigations and emphasized that the deceased's medical privacy and dignity remain protected under China's Civil Code, Cybersecurity Law, and the PIPL. According to Chinese legal commentary, lawyer Xu Hao in the China Daily newspaper on 15 December 2023, following the Kathy Chow medical records leak incident, stated: 'The unauthorized disclosure of the medical data … is disrespect-

ful and a violation of [the deceased's] privacy', and relatives may initiate civil proceedings to seek compensation.

As evidenced by these decisions, Chinese courts protect the reputation and private interests of deceased individuals, permitting close relatives to sue when a loved one's dignity or memory is harmed. Empirical work by scholars such as Bo Zhao (2014) shows that courts have accepted dozens of such claims, demonstrating a consistent judicial willingness to defend posthumous reputation and privacy. Further, Wang X. (2022) affirms this, saying 'The bundle of personal information rights … falls under the paradigm of individual autonomy and control.' More recently, Chinese regulators and internet courts have begun addressing emerging issues such as AI-driven digital resurrection and the creation of posthumous digital replicas. Emily Feng's article published on NPR media outlet titled '*Chinese Companies Offer to Resurrect Deceased Loved ones with AI Avatars*' on 21 July 2024 confirms this. Together, these developments illustrate that China has an established and growing legal architecture that recognizes posthumous privacy as an extension of personality rights and family dignity.

Key learnings from China are: China's *Personal Information Protection Law (PIPL), 2021* offers Kenya an exceptionally useful comparative model because it expressly addresses the personal information of deceased persons. Article 49 permits close relatives, for their own lawful and legitimate interests, to exercise rights of access, copying, correction, and deletion concerning the deceased's personal information, subject to the deceased's prior arrangements.

Noteworthy is that posthumous data privacy in China applies both in testacy and intestate scenarios. Laws seamlessly fall into place whether the deceased had wishes in a will or not; hence, there is no gap. Lastly, China's model also demonstrates that posthumous protection can be limited and structured, rather than creating an unlimited continuation of all privacy rights after death.

Guided by the foregoing jurisprudence from Rwanda and China, Section V of this paper proposes recommendations for protecting posthumous data in Kenya.

V. PROTECTING POSTHUMOUS DATA IN KENYA

Kenya's DPA 2019 is progressive in safeguarding the rights of living data subjects, yet it contains a significant gap: it has no clear recognition nor protection of the data of individuals after death. This paper does not push for Kenya to copy foreign legislative models word for word, lest law reformers fall into the trap of *transplanting an English oak in Africa* - imposing foreign laws in a bid to resolve local legal problems. Rwanda allows people to decide, while they are alive, who can manage their personal data after they die. Article 25 of Rwanda's Law No 058/2021 says personal data is not inherited, but someone can use it to give processing rights to an heir by will. On the other hand, China uses a broader legal rule. Article 49 of its Personal Information Protection Law allows close relatives, acting in their own legal interests, to exercise certain rights regarding a deceased person's personal information, unless the person had made other arrangements while alive.

These examples offer Kenya a key lesson evident from the recommendations proposed herein: protecting data after death should not be handled like regular inheritance, nor does it mean that privacy rights last forever. Rwanda's approach focuses on honoring the clear wishes of the deceased, while China's model shows the value of having a legal default when there are no instructions. Posthumous privacy reform needs to reflect on the country's political and institutional context too. Parliamentarians engaged in a stakeholder approach can bridge this gap. Legal reforms and amendments require political goodwill in Parliament, without which it is a challenge. Reforms should be part of a wider review and amendments of the DPA, 2019. This approach makes it more likely that Parliament will consider the changes. Notably, before any reforms, the Office of the Data Protection

Commissioner should lead consultations with stakeholders such as healthcare and financial institutions, archives, digital platforms, civil society, academics, and families who are affected. Recommendations for amending the DPA, 2019 to cover gaps are highlighted below.

Asta Tūbaitė-Stalauskienė (2018) observes that there are difficulties surrounding post-mortem protection of personal data, especially stemming from exclusion of deceased persons from the legal framework. First, expand the definition of a 'data subject'. In light of Asta's argument, *Section 2 of the DPA, 2019* is the cornerstone of the entire legislative scheme. Amend section 2 by introducing a supplementary definition that recognizes deceased individuals as falling within the protective scope of the Act for specified purposes.

Proposed wording: *For the purposes of Parts V, VI, and VIII of this Act, where a data subject is deceased, references to the data subject shall be construed to include an authorized representative or heir of the deceased, acting in that capacity.*

Second, introduce a framework for posthumous privacy data. Sections 26 and 27 of the DPA, 2019 set out rights available to data subjects: the right of access to personal data, the right to request rectification of inaccurate data, the right to erasure, the right to object to processing, and the right to restriction of processing, among others. The amendment proposed, first, is introducing a subsection to section 26 of the DPA, 2019 providing the rights of access, erasure, and restriction of processing survive the death of the data subject and may be exercised by authorized representatives or heirs.

The subsection should also specify that such exercise of rights is subject to any overriding legal, public interest, or archival considerations that may apply in a given case, a necessary qualification that prevents the posthumous rights framework from becoming a mechanism for suppressing historically significant or legally relevant information. Proposed wording:

Where a data subject is deceased, the rights conferred by this section may be exercised by the data subject's legal representative, executor, administrator of the estate, or a person designated by the data subject during their lifetime for this purpose. Such exercise shall be subject to any legal obligations, public interest considerations, or archival purposes that may lawfully restrict those rights.

The second is a new standalone section proposed as *section 33B* dedicated to the processing of posthumous personal data, which would establish the framework within which such processing may take place and the safeguards that must attend it.

A new Section 33B should be framed as a comprehensive provision governing the treatment of posthumous personal data. It should establish: (i) a general prohibition on the processing of the deceased's personal data except on specified lawful grounds; (ii) a requirement that data controllers take reasonable steps to identify and flag personal data belonging to deceased individuals upon notification of death; (iii) minimum retention and deletion standards for such data; and (iv) the rights of authorized representatives to request information, rectification, deletion, or restriction in respect of that data. The section should further make provision for the recognition of *ante-mortem instructions*, that is, instructions given by a data subject during their lifetime regarding the posthumous handling of their personal data, and should require data controllers to honor such instructions to the extent practicable.

Third, clarify the lawful grounds for processing posthumous data. Section 30 of the DPA, 2019 prescribes the lawful grounds upon which personal data may be processed. Further, *Data Protection (General) Regulations 2021,* regulation 5 and regulation 29 also require lawful bases. In the posthumous context, several existing grounds remain relevant and capable of application, in particular, compliance with a legal obligation, the performance of a public interest task, and historical or research purposes.

The recommendation is to introduce additional subsections to Section 30 that address the posthumous context specifically. These should make clear, first, that the processing of a deceased individual's personal data for commercial purposes, including advertising, profiling, or sale of the data, is not a lawful ground of processing unless the deceased gave express consent during their lifetime or their authorized representative gives such consent after death. Second, the amendments should recognize that processing for legitimate historical, archival, journalistic, or academic research purposes may proceed without the consent of an authorized representative, subject to the data minimization principle and appropriate safeguards for dignity and reputation. Third, the processing of posthumous data to administer an estate, to comply with a legal or regulatory obligation, or to resolve a legal dispute should be expressly recognized as a lawful ground.

Fourth is accountability for Controllers and Processors. The accountability regime established by Sections 25 to 48 of the Act imposes on data controllers and processors a comprehensive set of obligations: to process data lawfully, fairly, and transparently; to collect data only for specified and legitimate purposes; to ensure accuracy; to limit retention; and to implement appropriate security measures. When there is no living data subject, data controllers and processors are left without clear guidance on how to discharge their accountability obligations. The recommendation under this heading is to introduce an explicit provision appropriately located within Part IV or as a new Part IVA that sets out the specific accountability obligations of data controllers and processors in relation to posthumous personal data.

Those obligations should include, at minimum: a duty to maintain records identifying personal data held in respect of deceased individuals, updated upon notification of death; a duty to implement procedures for responding to requests from authorized representatives; a prohibition on the commercial exploitation of posthumous personal data without explicit consent; a duty

to take reasonable steps to ensure the accuracy and appropriate restriction of posthumous data; and a prohibition on the public dissemination of sensitive posthumous personal data, including health information, intimate images, and biometric data, where no lawful ground exists and where such dissemination would cause harm to the dignity of the deceased or distress to their surviving family. Under the DPA, 2019, no explicit legal barrier exists to prevent them from monetizing it. That is a gap that requires direct legislative attention.

Fifth, strengthen the enforcement framework for posthumous data. Although Part VIII of the DPA empowers the ODPC to investigate complaints, conduct audits, issue enforcement notices, and impose financial penalties, these powers are currently limited to protecting the rights of living data subjects. Consequently, families of deceased persons whose personal data, such as medical records or private photographs, has been unlawfully disclosed have no clear legal avenue to seek redress under the Act. To address this gap, the law should expressly permit authorized representatives or heirs to lodge complaints relating to breaches of posthumous data rights. The ODPC should also be empowered to investigate such complaints, order the deletion or removal of unlawfully processed data, issue enforcement notices, impose financial penalties, and, where necessary, obtain injunctions to prevent continued misuse of a deceased person's personal data. Where no authorized representative exists, the ODPC should have the authority to act on its own in the public interest, particularly where sensitive data may harm surviving relatives or other vulnerable persons.

Lastly, develop subsidiary guidance on posthumous data governance. Legislative reform alone cannot resolve every practical issue surrounding deceased persons' personal data. The Cabinet Secretary and the ODPC should therefore issue regulations and *Posthumous Data Privacy Guidance Notes* addressing matters such as proof of representative authority, data retention periods, procedures for handling competing family claims,

complaint mechanisms, and best practices for organizations that routinely process personal data, including healthcare providers, financial institutions, and social media platforms. Such guidance would promote consistency, legal certainty, and responsible management of posthumous data.

VI. CONCLUSION

Posthumous data will always be a part of society and life. Natasha Chu (2015) affirms that when the law remains silent on posthumous data, the information of the deceased is left exposed to interpretation, discretion, and potential misuse. Kenya's ODPC should incorporate the recommendations above into privacy regulation by anchoring its approach in the Dignity theory and Autonomy theory discussed earlier.

The preceding analysis establishes that posthumous data privacy is an important yet substantially underdeveloped tenet of Kenyan data-protection law. The DPA, 2019 adopts a framework focused on the 'data subject' as an identified or identifiable natural person and defines personal data accordingly - an approach that results in a notable legal gap upon the death of the data subject. Further, the DPA, 2019 does not explicitly clarify whether, or to what extent, personal data remains protected after death, nor does it provide a comprehensive framework specifying who may exercise rights over a deceased person's data, for what purposes, and under what limitations.

This current Kenyan posthumous data legal gap generates uncertainty regarding the source, scope, duration, and enforcement of such protection. This issue is especially pertinent given that health records, biometric data, photographs, correspondence, social-media content, genetic information, financial records, and other digitally stored information may persist for decades after an individual's death. The absence of an explicit statutory framework increases the risk of inappropriate disclo-

sure, exploitation, or continued processing of such information, just to mention a few abuses.

The comparative analysis in this paper provides law reformers access to legislative models that could inform potential reforms. Rwanda offers a particularly relevant regional example. China authorizes close relatives of a deceased natural person, for their own lawful and legitimate interests, to exercise specified rights over the deceased's personal information, including consultation, copying, correction, and deletion, unless the deceased made alternative arrangements during life.

This paper implores the Kenyan legislature to amend the DPA, 2019 as guided by the recommendations. As argued above, the law ought to empower individuals, while alive, to determine the posthumous handling of their personal data while establishing a default mechanism in the absence of such instructions. Accordingly, authorized representatives should be required to demonstrate a legitimate interest and exercise rights subject to necessity, proportionality, confidentiality, and the rights of living third parties. Reform should also establish clear rules for sensitive categories of information, such as health, genetic, biometric, financial, and family data. Special safeguards are warranted where disclosure could impact surviving relatives or other living individuals. Alive to challenges like political and institutional goodwill, robust public participation and stakeholder engagement would cure the issues. Kenya's constitutional commitment through Articles 28 and 31 to dignity and privacy respectively, and the protection of individual rights, offers a robust normative basis for posthumous data reforms. Acknowledging that this paper is not exhaustive and merely guiding towards posthumous data privacy reforms, this paper suggests future research areas.

Additional research is warranted on digital inheritance, social media accounts, genetic and family data, posthumous health records, deceased persons' biometric information, and the evidentiary challenges involved in establishing unlawful disclosure after death. Comparative jurisprudence research should encom-

pass jurisdictions beyond Rwanda and China that have adopted alternative models of posthumous data protection, like Germany. Additionally, empirical research should examine the perspectives of families, healthcare institutions, digital platforms, data controllers, the ODPC, archivists, and legal practitioners regarding the appropriate duration, beneficiaries, and limitations of posthumous data rights. This paper argues that the objective of reform is not to establish an unlimited 'right to privacy after death', but rather to create a principled, constitutionally grounded, and administratively feasible framework for the ongoing protection of personal data after death. Such a framework would address a clear gap in Kenya's posthumous data-protection architecture while safeguarding the legitimate interests of surviving individuals, society, research, historical preservation, and lawful data processing.

REFERENCES

Ajemian v. Yahoo! Inc. Massachusetts Supreme Court (2017).

Allen Waiyaki Gichuhi & Charles Wamae v. Florence Mathenge & Ambrose Waigwa (2022) eKLR HC Nairobi.

Anatomy Act, Cap. 249.

Births and Deaths Registration Act, Cap 149.

Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. New York University Law Review, 39(6), 962–1007.

Bloustein, E. J. (2009). Privacy as an aspect of human dignity: An answer to Dean Prosser. In F. D. Schoeman (Ed.), Philosophical dimensions of privacy (pp. 156–202). Cambridge University Press. (Original work published 1984)

Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. Ethics and Information Technology, 19(2), 129–142. https://doi.org/10.1007/s10676-017-9421-9

China's Personal Information Protection Law, 2021.

Computer Misuse and Cybercrimes Act, 2018.

Constitution of Kenya, 2010.

Čtvrtník, M. (2023). Personality rights, privacy, and post-mortem privacy protection in archives: International comparison, Germany and 'protection of legitimate interests.' In Archives and Records (pp. 115–134). Palgrave Macmillan.

Data Privacy and Governance Society of Kenya, January 2025 Report on ODPC Determinations in 2024 Analysis Report p.3; Nairobi.

Data Protection (General) Regulations 2021.

Data Protection Act, 2019.

Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Case C-311/18), ECLI:EU:C:2020:559. Schrems II.

Davey, T. (2020). Until death do us part: Post-mortem Privacy Rights for the Ante-mortem Person (Doctoral thesis, University of East Anglia). UEA Digital Repository. https://ueaeprints.uea.ac.uk/id/eprint/79742/

Deepa Jayakumar v. A.L. Vijay (2021) Madras High Court-Div. Bench.

Dickson Mwangi Munene v. Nyamega Gisesa & Nation Media Group Civ. Appeal. 369 of 2019 [2025].

Donald Kipkorir v. Muthaiga Country Club Plc. & 8 Others E455 of 2024 [2025].

Dr. A Shaji G., Mamedova S. (2024) Digital Afterlife: Preserving Online Legacies Beyond Death; Partners Universal International Innovation Journal Vol: 02 Issue: 01 January-February 2024. ISSN: 2583-9675 pp.4-5.

Dworkin, R. (2011). Justice for Hedgehogs (pp. 255–327). Belknap Press of Harvard University Press.

Edina Harbinja. (2022/2023). Digital death, digital assets and post-mortem privacy: Theory, technology and the law. Edinburgh University Press.

Ephraim Kenyanito and Sigi Mwanzia, 'Speaking from the Grave: Death, Data Protection under Kenyan Law' *The Star* (13 April 2021) https://www.the-star.co.ke/in-pictures/2021-04-13-speaking-from-the-grave-death-data-protection-under-kenyan-law/ accessed 17/07/2026.

France fines Google USD 170 Million and Facebook USD 68 Million over Cookie Consent Violation-DATA SECURE https://www.datasecure.ind.in/blogs/france-fines-google-usd-170-million-and-facebook-usd-68-million-over-cookie-consent-violation/

Fried, C. (1970). Privacy (pp. 7–8, 25–28, 32–33). Harvard University Press.

Garner B. (ed.) (2019) Black's Law Dictionary 11th edition.

Germany's Census Case (1983) BVerfGE 65, 1-Census Case (Volkszählungsurteil), Federal Constitutional Court of Germany.

González Fuster, G. (2014). The emergence of personal data protection as a fundamental right of the European Union. Springer. https://doi.org/10.1007/978-94-017-7546-6

Harbinja E. (2022) Digital Death, Digital Assets and Post-Mortem Privacy: Theory, Technology and the Law. Edinburgh University Press.

Harbinja, E., Legal Aspects of Transmission of Digital Assets on Death (Routledge 2017) 66–88.

Hollis, D., & Tikk, E. (2022). Peaceful Settlement in International Law. Texas International Law Journal, 57(2), 133-183.

Hongladarom, S. (2016). Philosophical foundations of privacy. In A Buddhist Theory of Privacy. Springer Briefs in Philosophy. Springer, Singapore.

K.S. Puttaswamy v. Union of India (2017) Supreme Court of India.

Kant, I. (1996). Groundwork of the metaphysics of morals (M. J. Gregor, Trans., pp. 37–49). Cambridge University Press. (Original work published 1785)

KICTANet. (2018/2021, September 12). What should happen to personal data when someone dies? KICTANet. https://www.kictanet.or.ke/what-should-happen-to-personal-data-when-someone-dies/

L. Edwards & E. Harbinja. (2013). Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. Cardozo Arts & Entertainment Law Journal, 32(1), 101–147.

Law of Succession Act, Cap 160.

Maximillian Schrems v Data Protection Commissioner (Case C-362/14), CJEU (2015).

McCallig, D. (2014). Dead right? The privacy of the deceased in post-mortem privacy. Computer Law & Security Review, 30(2), 153–162. https://doi.org/10.1016/j.clsr.2014.01.010

Mill, J. S. (1978). On liberty (E. Rapaport, Ed., pp. 9–33). Hackett Publishing Company. (Original work published 1859)

MWK & Ano. v. Attorney General & 4 Others [2017] KEHC.

Naomi Cahn, Dead Hands, Data and Digital Assets: The Law of the Digital Afterlife (2019) 25 Stanford Journal of Law, Business & Finance 175 pp.178-185.

Natasha, C. (2015). Protecting privacy after death. Northwestern Journal of Technology and Intellectual Property, 13(2), Article 8.

Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, (2nd Chamber) 19th October, 2016, ECLI:EU:C:2016:779.

Penal Code, Cap. 63.

Posner, R. A. (1981). The economics of justice (pp. 233–249). Harvard University Press.

Public Health (Public Mortuaries) Rules, 1991.

Public Health Act Cap.242.

Rachels, J. (1975). Why privacy is important. Philosophy & Public Affairs, 4(4), 323–333.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 (Regulation (EU) 2016/679). https://gdpr-info.eu

Republic v Joe Mucheru, Cabinet Secretary Ministry of Information Communication and Technology & 2 others; Katiba Institute & another (Ex parte); Immaculate Kasait, Data Commissioner (Interested Party) [2021] KEHC 122 (KLR).

Republic v. Naftali Njami Kinuthia [2019] High Court of Kenya 6559 (KLR)

Rosen, J. (2000). The unwanted gaze (pp. 8–14). Random House.

Rössler, B. (2005). The value of privacy (R. D. V. Glasgow, Trans.). Polity Press.

Rupniewski, M. (2023). Human dignity and the law: A personalist theory. Routledge.

Rwanda Law No.058/2021 on the Protection of Personal Data and Privacy.

S v Makwanyane and Another (CCT3/94) [1995] ZACC 3,

Scarre, G. (2012). Privacy and the dead. Philosophy in the Contemporary World, 19(1), 1–16. https://doi.org/10.5840/pcw201219112

Sentinel Africa Consulting. (2024). The Data Protection Act and deceased individuals' privacy. https://sentinelafricaconsulting.com/data-protection-deceased/

Solove, D. J. (2002). Conceptualizing privacy. California Law Review, 90(4), 1088–1154.

Solove, D. J. (2008). Understanding privacy. Harvard University Press.

Stored Communications Act. (US)

Tosoni, L., & Bygrave, L.A. (2020). Article 4 Definitions. Oxford University Press E-Books. https://doi.org/10.1093/oso/9780198826491.003.0006

Tūbaitė-Stalauskienė, A. (2018). Data protection post-mortem. International Comparative Jurisprudence, 4(2), 97–104. https://doi.org/10.13165/j.icj.2018.12.003.

Wacks, R. (2013). Privacy and media freedom (pp. 22–36, 96–112). Oxford University Press.

Wang, X. (2022). The bundle of personal information rights from the perspective of state protection. Social Sciences in China, 43(2), 36–54. https://doi.org/10.1080/02529203.2022.2093062

Webber v. Information Commissioner and Cabinet Office [2017] UKUT 312.

Westen, P. (1982). The empty idea of equality. Harvard Law Review, 95(3), 537–596.

Westin, A. F. (1967). Privacy and freedom (pp. 7–12, 31–33). Atheneum Press.

Yash Pal Ghai & Jill C. Ghai. (2019, January 25). Katiba: The state of human rights and freedoms in Kenya. The Star. https://www.the-star.co.ke/sasa/lifestyle/2018-12-08-katiba-the-state-of-human-rights-and-freedoms-in-kenya

Zhao, Bo. (2014). Posthumous reputation and posthumous privacy in China: The dead, the law, and social transition. Brooklyn Journal of International Law, 39(1). https://ssrn.com/abstract=2724317

Zimmer, V. (2021). Winter is Here: The Impossibility of Schrems II for U.S.-Based Direct-to-Consumer Companies. Northwestern Journal of International Law & Business, 42(1), 75-116.

JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 6, Issue 1 (2026) p.59-100
https:doi.org/10.52907/jipit.2026.609

Fortifying the Digital Frontier: An Analysis of Legal and Technical Frameworks for Data Systems Resilience in Kenya

*Martin Mungai**

ABSTRACT

Kenya's Data Protection Act (2019) is routinely treated, in public commentary and in regulatory practice, as the statute answerable for the country's cyber resilience failures. This paper argues that the treatment is misplaced, and that correcting it clarifies where Kenya's resilience deficit actually sits and how to address it. Kenya already possesses a prescriptive resilience regime. Gazette Notice No. 1043 of 31 January 2022 designated telecommunications, health, banking, and 11 other sectors as critical information infrastructure under the Computer Misuse and Cybercrimes Act (2018), and the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations (2024) attach measurable obligations to that designation, including annual risk assessment against defined recovery time objectives, mandatory disaster recovery sites, annual audit by an auditor appointed by the Director, and incident reporting within 24 hours. Those obligations bind the owners of designated infrastructure only once a supervisory institution exists to receive, audit, and act on what they require, and regulation 11 of the 2024 Regulations places that duty on each sector regulator without providing it any funding to discharge it. Drawing on the 2023 eCitizen outage, the November 2025 defacement of government websites, the October 2025 M-Tiba breach, and recurring outages on the M-Pesa network, this paper shows that these obligations have been operationalized in one sector only, banking, where the Central Bank of Kenya has both licensing leverage and a funded Sector

* Martin Mungai holds an MPhil in Advanced Computer Science from the University of Cambridge and is a Certified Information Systems Auditor (CISA) and Certified Information Security Manager (CISM). He is an ICT Consultant at Les Conseillers Kenya Ltd., Nairobi, where he advises on information systems governance, audit and cybersecurity. ORCID: 0009-0009-4328-0608. Email: mungai.martin@theconsultantske.com

Cybersecurity Operations Centre. Therefore, the deficit is institutional rather than legislative. This paper identifies one genuine drafting gap alongside this institutional failure, namely the absence of a testing and evaluation duty in section 41(4) of the Data Protection Act (2019), and proposes a reform agenda sequenced by institutional difficulty.

Keywords: Data Protection, Information Technology, Legal Liability, System Resilience, Technology Law

TABLE OF CONTENTS

ABSTRACT 59
I. INTRODUCTION 61
II. SECURITY IS NOT RESILIENCE 65
A. *Two Different Engineering Problems* 65
B. *What the Data Protection Act Actually Requires* 66
C. *The Case for Technology-Neutral Drafting, and Where it Runs Out* 68
III. THE RESILIENCE REGIME IN KENYA 69
A. *The Statutory Architecture and the Fact of Designation* 69
B. *The Obligations that Designation Triggers* 71
C. *Constitutional Limits on Expanding the Framework* 74
IV. FOUR DESIGNATED SECTORS, ONE FUNCTIONING CHAIN 76
A. *Finance: What Implementation Looks Like* 76
B. *Health: The Same Obligations without the Institution* . 79
C. *E-Government: The Same Statutes, Divergent Outcomes* 82
D. *Telecommunications: Designated, Disrupted, Undocumented* 84
V. THE ENFORCEMENT ASYMMETRY AND ITS CAUSES 87
A. *An Active Regulator, Active in One Direction* 87
B. *Fiscal Capacity Across a Multiagency Framework* 88
VI. A SEQUENCED REFORM AGENDA 90
A. *Phase One: Administrative Coordination* 90
B. *Phase Two: Subsidiary Regulation and Sectoral Build-Out* 91
C. *Phase Three: Legislative and Fiscal Commitments* 93
VII. CONCLUSION 94

I. INTRODUCTION

Kenya's position as East Africa's technology hub is not merely a marketing claim. By the end of 2024, the country had 66.1 million mobile network connections, with a penetration rate above 100%, and more than 5,000 government services running through a single portal, eCitizen (GSMA, 2024; World Bank, 2023). The Global System for Mobile Communications Association projects that the digital economy will contribute roughly 662 billion Kenyan Shillings to Gross Domestic Product (GDP) by 2028 (GSMA, 2024), and the World Bank backed that trajectory with a 390 million United States Dollar commitment to the Digital Economy Acceleration Project in 2023 (World Bank, 2023).

What has changed faster than the institutions is the shape of the threat. The National Kenya Computer Incident Response Team Coordination Centre (National KE-CIRT/CC), operated by the Communications Authority of Kenya, recorded approximately 4.5 billion cyber threat events between April and June 2025, an increase of roughly 80% on the previous quarter, with distributed denial-of-service attempts rising by 255.6% (Communications Authority of Kenya [CA], 2025b). Two qualifications are necessary, however. The Authority itself attributes the increase principally to an upgrade of KE-CIRT tools that widened its surveillance rather than to a proportionate rise in adversary activity (CA, 2025b), and detections fell to approximately 842 million in the following quarter (CA, 2026a). The aggregate figures are therefore a poor measure of trend, though what they do establish reliably is the character of the threat: for the most part these are not break-ins aimed at stealing a database, but attempts to halt a system's functioning, through distributed denial-of-service floods against government portals, ransomware against hospitals, and defacement campaigns against ministries.

Two questions must be separated before the threat picture can be turned into a legal argument, and much of the existing Kenyan commentary does not separate them. The first is whether Kenyan law contains obligations directed at system resilience,

as distinct from data privacy. The second is whether those obligations are enforced. The answer to the first question has been affirmative since January 2022. The answer to the second is that they have been enforced in one designated sector only.

This distinction matters because the prevailing framing gets it the wrong way round. When the mobile health wallet M-Tiba was breached in October 2025, exposing records relating to some 4.8 million people, the regulator that responded publicly was the Office of the Data Protection Commissioner (ODPC), acting under the Data Protection Act (2019) (Streamlinefeed, 2025). Contemporaneous reporting framed the incident as a test of Kenya's data protection framework and as a potential violation of the Data Protection Act's breach notification timeline (TechCabal, 2025b; Streamlinefeed, 2025). Health had, at that point, been a designated critical information infrastructure sector for more than three years, by virtue of Gazette Notice No. 1043 of 31 January 2022, issued under section 9 of the Computer Misuse and Cybercrimes Act (2018) (CMCA) (National Computer and Cybercrimes Co-ordination Committee [NC4], 2022). There is no comparable public record of a response by the National Computer and Cybercrimes Co-ordination Committee (hereafter 'the Committee'), which is the body that the statute charges with critical infrastructure protection.

It is not in doubt that the Committee is capable of responding when it chooses to. Three weeks after the M-Tiba breach, when government ministry websites were defaced, the public statement came from the Principal Secretary for Internal Security, who chairs the Committee, directing the public to report suspicious activity to the National KE-CIRT/CC, the Committee and the Directorate of Criminal Investigations (State Department for Internal Security and National Administration, 2025). That statement is also instructive on the framing question, because it characterized the attack as a breach of the Computer Misuse and Cybercrimes Act, the Kenya Information and Communications Act and the Data Protection Act together (State Department

for Internal Security and National Administration, 2025). The government therefore treats the three instruments as jointly engaged by a resilience incident, which is the correct position and which the analysis below adopts.

The observation that the Data Protection Act (DPA) carries more weight in this area than its own text supports is not novel. In a joint analysis submitted shortly after the Act's commencement, the Defenders Coalition, the Kenya Legal and Ethical Issues Network on HIV and AIDS, Dr Robert Muthuri and Privacy International noted that section 25, which sets out the principles of data protection, omits integrity and confidentiality altogether, that the principle appears only in sections 41 and 42, and that this inconsistency is confusing (Defenders Coalition et al., 2020). The same analysis observed that section 23, which empowers the Data Commissioner to audit the systems of controllers and processors, contains no criteria governing when that power should be exercised, and urged the Commissioner to publish guidelines on the point (Defenders Coalition et al., 2020). Both observations have proved durable. A subsequent multistakeholder review marking five years of the Act reached a similar conclusion from the institutional side, identifying limited funding, low staffing, the ODPC's legal structure and the existence of competing data protection frameworks as the principal obstacles to implementation, and urging Parliament to make the Office autonomous of the parent ministry and to increase its allocation (KICTANet, 2024).

The problem this paper addresses is therefore neither a missing statute nor, principally, a defective one. It is an institutional failure with two components. The first is that Kenya's prescriptive resilience regime, which binds owners of designated critical information infrastructure, has been operationalized in a single sector. The second concerns those who fall outside that regime. The CMCA binds everyone in the sense that its offense provisions apply generally, but the prescriptive resilience duties examined in this paper are triggered by designation under sec-

tion 9 and attach only to owners of designated critical information infrastructure. An organization that has not been designated is therefore governed, so far as resilience is concerned, by the DPA alone, and that statute contains no obligation a regulator can objectively test, because it omits the one drafting feature, a duty to test and evaluate, that makes a technology-neutral security standard enforceable.

The analysis advanced in this paper is doctrinal. It works from the text of the Data Protection Act (2019), the Computer Misuse and Cybercrimes Act (2018) as amended in 2025, their subsidiary regulations, and the gazette notices issued under them, read against documented incidents drawn from regulatory publications, court records, and contemporaneous reporting. The author also employs Article 32(1)(d) of the European Union's General Data Protection Regulation (GDPR) as a drafting comparator, because section 41(4) of the Data Protection Act borrows the surrounding language of Article 32 closely while omitting that subparagraph. It is used to isolate a specific textual feature, not as a general comparative survey.

Part II of this study distinguishes data security from system resilience, sets out precisely what the Data Protection Act requires, and identifies the single drafting gap that matters. Part III turns to the Computer Misuse and Cybercrimes Act (2018) and the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024, showing that the prescriptive obligations Kenyan commentary treats as absent are actually in force, and that the two statutes are designed by their own terms to operate together rather than severally or in competition. It also examines the constitutional limits the courts have recently placed on the expansion of the Committee's coercive powers. Part IV tests the core argument of this paper against four sectors: finance, where the framework has been implemented; health, where it has not; e-government, where the same statutes produced divergent outcomes within a single attack; and telecommunications, where a designated sec-

tor has generated repeated disruption without any public technical accounting. Part V examines why enforcement has been asymmetric, locating the cause in the distributed fiscal capacity of a multiagency framework rather than in the shortcomings of any single regulator. Part VI sets out a reform agenda sequenced by institutional difficulty. Part VII concludes this paper.

This paper does not attempt a comprehensive treatment of every designated sector. The four sectors examined are selected because each produced a documented resilience incident within the past three years suitable for close analysis. As a result, energy, transport and electoral systems, all named in Gazette Notice No. 1043, fall outside its scope.

II. SECURITY IS NOT RESILIENCE

A. Two Different Engineering Problems

Data security and system resilience are frequently treated as synonyms in Kenyan policy discourse, and the conflation has consequences for how obligations are read. Data security is a preventive discipline: firewalls, access controls, and the encryption of data at rest, in transit, and in use, all aimed at keeping an unauthorized actor out of a system entirely. It maps onto the control-oriented and risk-management principles embodied in ISO/IEC 27001, which specifies requirements for establishing, maintaining, and continually improving an information security management system (International Organization for Standardization [ISO], 2022), and it assumes, reasonably enough for many threats, that a digital perimeter can be defended.

System resilience begins from the opposite assumption. It assumes that the perimeter will eventually be breached and asks what happens next. Can the system detect the intrusion quickly? Can it fail over to redundant infrastructure rather than going dark? Can it restore from backups that the attacker could not also encrypt or delete? These are the questions addressed by business

continuity frameworks, most notably ISO 22301, which specifies requirements for a management system to protect against, reduce the likelihood of, prepare for, respond to, and recover from disruptions (ISO, 2019). The distinction tracks that drawn in the engineering literature between resisting an adverse event and adapting to and recovering from one (National Institute of Standards and Technology [NIST], 2021). It is a fundamentally different engineering problem from access control. A system can be, on paper, fully compliant with every data security obligation in the DPA and still collapse the moment it is attacked, because nothing in that compliance regime requires it to have a tested failover plan.

The M-Tiba breach clearly illustrates this distinction. CarePay Limited, which operates the platform, received ISO/IEC 27001:2022 certification for its information security management system in August 2025, two months before the intrusion (TechCabal, 2025a). The certification was not fraudulent, and the security architecture was not absent, yet the intrusion nonetheless ran from 17 to 25 October 2025 and was not discovered until 27 October 2025, a detection gap of ten days (TechCabal, 2025b). Certified security architecture is simply not the same thing as tested resilience.

B. What the Data Protection Act Actually Requires

Precision about the statutory text is necessary here, because the DPA is regularly credited with data security provisions it does not contain.

Section 25 of the DPA sets out the principles of data protection, requiring, among other things, that personal data be processed in accordance with the right to privacy, lawfully and transparently, for explicit and legitimate purposes, and that it not be transferred outside Kenya unless there is proof of adequate safeguards or the data subject's consent. Notably, section 25 does not contain a security principle: integrity and confiden-

tiality, which appear as a principle in comparable statutes, are absent from section 25 and appear instead as obligations in sections 41 and 42 (Defenders Coalition et al., 2020).

Section 41 of the DPA imposes data protection by design and by default, obliging controllers and processors to implement appropriate technical and organizational measures. Subsection (4) offers illustrations: identifying reasonably foreseeable risks, establishing safeguards against them, pseudonymization and encryption, and the ability to restore availability and access in a timely manner. Section 42 supplies the factors relevant to determining what is appropriate, directing the controller to have regard to the state of technological development available, the cost of implementing security measures, and the special risks that exist in the processing. Section 43 requires notification to the ODPC within 72 hours where there is a real risk of harm to a data subject.

Two further provisions are relevant and are usually overlooked. Section 23 empowers the Data Commissioner to carry out periodical audits of the processes and systems of controllers and processors to ensure compliance with the DPA, while section 50 empowers the Cabinet Secretary to prescribe, on grounds of the strategic interests of the state or the protection of revenue, categories of processing that may be effected only through a server or data center located in Kenya. The DPA, in other words, already contains both an audit power and a localization power, though neither has generated a published body of practice.

Read together, these provisions describe a compliance regime built around lawful processing, transparency, and post-incident notification. They do not specify a testing cadence, a recovery time objective, or a minimum standard for what 'appropriate' means in any sector. An organization can therefore satisfy the DPA in full while operating infrastructure with no tested backup, no segmented network, and no incident response plan beyond the 72-hour notification clock, because the statute does not require those measures.

C. The Case for Technology-Neutral Drafting, and Where it Runs Out

There is a serious argument for the generality of section 41, and it deserves to be taken on its own terms rather than dismissed. Technology-neutral drafting is standard legislative practice precisely because prescriptive technical mandates date quickly. A statute that named specific encryption algorithms or firewall configurations in 2019 would already be obsolete by 2026. There is also a fairness dimension. Kenya's controller population includes a very large number of small and medium enterprises for which a mandatory zero-trust architecture or a quarterly third-party penetration testing regime would be a real and disproportionate cost. Therefore, by directing attention to the cost of implementation, section 42 expressly builds that proportionality into the standard.

The difficulty is that this argument justifies flexibility in how a standard is met. It does not justify the absence of any obligation to demonstrate that the chosen measures work. The distinction becomes visible when a jurisdiction with an equally technology-neutral standard actually enforces it.

In the United Kingdom, British Airways suffered a compromise between 22 June and 5 September 2018 in which an attacker diverted customer traffic to a fraudulent site and harvested the personal and payment card data of approximately 430,000 customers and staff. The airline did not detect the compromise itself; it was alerted by a third party more than two months later (Ropes & Gray, 2020). The Information Commissioner's Office ultimately imposed a penalty of 20 million pounds in October 2020, reduced from a notice of intent of 183 million issued the previous year, finding that the airline had processed a significant volume of personal data without appropriate security contrary to Articles 5(1)(f) and 32 of GDPR (Faegre Drinker Biddle & Reath, 2020; Ropes & Gray, 2020). The regulator's reasoning did not turn on the airline's choice of technology. It turned on the existence of measures that were available, inexpensive and un-

implemented, and on the fact that it was unclear whether British Airways would ever have detected the compromise on its own (Faegre Drinker Biddle & Reath, 2020).

That last finding is the one that matters here. Article 32(1)(d) of the GDPR requires controllers to maintain a process for regularly testing, assessing, and evaluating the effectiveness of their technical and organizational measures. Section 41(4) of the DPA lists substantially the same categories of measure but contains no equivalent duty. The consequence is not that Kenyan organizations are permitted weaker technology; it is that a Kenyan regulator investigating a comparable failure has no objective factual question available to it. A testing duty gives a regulator questions with determinate answers: 'Was a test conducted? When? By whom? What did it find?' A standard without one leaves only a normative question to be litigated after the event, namely 'whether the measure was appropriate', on which competent technical experts routinely disagree and which is correspondingly expensive to resolve.

This is not a minor drafting nicety. Given the capacity constraints discussed in Part V of this paper, it is the difference between a standard a regulator can afford to enforce and one it cannot. Therefore, technology neutrality is fully compatible with enforceability. What section 41(4) of the DPA demonstrates is that dropping the testing obligation while retaining the neutral language does not preserve flexibility so much as remove the feature that made the flexible standard workable.

III. THE RESILIENCE REGIME IN KENYA

A. The Statutory Architecture and the Fact of Designation

The Data Protection Act regulates the relationship between a controller and a data subject. It is largely silent on the relationship between a controller and an external attacker, because that was never its object. The CMCA is the statute written for that

relationship, and its institutional architecture is more developed than the Kenyan literature generally acknowledges.

Section 4 of the CMCA establishes the Committee. Section 6 of the CMCA sets out the functions of the Committee, which include advising the Government on security aspects of critical infrastructure, coordinating national security organs on computer and cybercrimes, and, at section 6(1)(e), developing a framework to facilitate the availability, integrity and confidentiality of critical national information infrastructure including telecommunications and information systems. Section 7 of the CMCA establishes the Secretariat and the office of the Director. Section 9 empowers the Director to designate systems as critical infrastructure by notice in the Gazette and sets the criteria for doing so. Section 10 addresses the protection of designated infrastructure, section 11 the reports owners must make, section 12 information sharing agreements, and section 13 the auditing of critical information infrastructure to ensure compliance.

Two features of the above list under the law deserve emphasis. Availability, the resilience property, is named in the statement of the Committee's functions under the CMCA. Further, an audit mechanism directed at compliance has existed in primary legislation since 2018.

Whether that architecture has been used is a separate question, and here a recurring assumption in Kenyan commentary is that the critical infrastructure provisions of the CMCA have lain dormant since enactment. That assumption is inaccurate. On 31 January 2022, exercising the powers conferred by section 9(1) and (2) of the CMCA, the Director designated systems across a range of sectors as critical infrastructure with effect from 20 January 2022, by Gazette Notice No. 1043. The designated sectors are telecommunications, electoral, judicial, education, health, food, water, land, energy, transport and industry, banking, finance, defense, security, and public safety. The designation (NC4, 2022) is confirmed in the National Cybersecurity Strategy 2022, which describes it as the step by which the Government

initialized critical information infrastructure protection as provided by the CMCA, covering systems whose disruption would interrupt life-sustaining services, adversely affect the economy, cause mass casualties, disrupt the money market, or severely affect national security (Ministry of Interior and National Administration, 2022).

Gazette Notice No. 1043 has since been relied upon as an operative instrument. In March 2024, the Communications Authority and the Committee jointly directed that all systems designated under it must use digital certificates and public key infrastructure services obtained exclusively from providers licensed by the Authority (CA, 2024).

B. The Obligations that Designation Triggers

What the CMCA left unspecified was the content of the obligations that designation triggers. That gap was filled on 16 February 2024, when the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024 were gazetted as Legal Notice No. 44, made under section 70 of the CMCA (Clyde & Co, 2024).

The Regulations set out the measures that section 41 of the Data Protection Act declines to name. Regulation 17 requires every owner of critical information infrastructure to conduct an annual cyber risk assessment and business impact analysis, to identify single points of failure, to implement business continuity controls including an information technology disaster recovery plan and a cyber incident response plan, and to base the business impact analysis on recovery time objectives, recovery point objectives, and maximum acceptable outage. Regulation 28 requires that infrastructure on which critical information is domiciled be located in Kenya, and provides that an owner wishing to locate it abroad must apply to the Committee, which must communicate its decision within 30 days of receiving the application. Regulation 31 sets out baseline security requirements,

including an internal cybersecurity policy reviewed at least annually, periodic testing and updating of business continuity and disaster recovery plans, annual cybersecurity risk assessment, annual internal cybersecurity audits, and participation in cybersecurity exercises and drills to verify readiness. Regulation 32 requires the designation of a Chief Information Security Officer. Regulation 42 requires the establishment of a disaster recovery and backup site in a location distinct from the main site. Regulations 44 to 50 establish the audit machinery: the Director appoints auditors, who may enter premises on 30 days' notice and require production of documents, and whose reports are tabled before the Committee, which issues recommendations that form the subject of evaluation in the following year's audit. Regulation 65(c) requires owners to report all cybersecurity incidents to the relevant Sector Cybersecurity Operations Centre within 24 hours of becoming aware of them.

The contrast with the general standard is not subtle: a localization requirement with a 30-day statutory clock is testable (either the infrastructure is in Kenya, or it is not), and an annual audit conducted by an auditor holding an appointment certificate is testable in a way that appropriate technical measures are not. Likewise, a recovery time objective is a number.

Because these obligations sit alongside those in the DPA, it is important to be exact about the relationship between the two regimes, since the argument that follows depends on it. The Data Protection Act and the 2024 Regulations are not alternatives, and a controller does not choose between them. The Regulations say so on their face. Regulation 31(1)(a)(ii) requires the internal cybersecurity policy of every designated owner to address data protection concerns consistently with the Data Protection Act. Regulation 74 provides that the Data Protection Act applies to the processing of personal data pursuant to the Act and the Regulations. A designated owner processing personal data is bound simultaneously and cumulatively by both instruments, and compliance with one neither satisfies nor excuses the other.

The division of labor the two instruments contemplate is functional rather than jurisdictional. The Data Protection Act allocates rights to data subjects and duties of lawfulness, transparency, and notification to controllers. The Computer Misuse and Cybercrimes framework allocates engineering duties to infrastructure owners and supervisory duties to the Committee and to sector regulators. Where a single incident engages both instruments, both apply. The failure in Kenya has not been that organizations have picked one regime over the other. It has been that only one half of the architecture has been built.

That cumulative operation is given institutional form through a structure of operations centers. The mechanism the Regulations rely on to make the audit and reporting obligations enforceable is a three-tier structure of Cybersecurity Operations Centres established by regulations 9 to 12: a National Cybersecurity Operations Centre, Sector Cybersecurity Operations Centres, and Critical Information Infrastructure Cybersecurity Operations Centres at the level of the individual owner.

Regulation 11(1) is the provision on which a great deal turns. It provides that the regulator of the sector in which the designated infrastructure is domiciled, or where applicable the relevant Ministry, shall be deemed to be the Sector Cybersecurity Operations Centre. Regulation 11(4) provides that the costs of operating each Sector Centre shall be borne by the regulator of that sector. The obligation on the owner to report within 24 hours under regulation 65(c) therefore presupposes the existence, in that owner's sector, of a regulator that has actually established and funded a Sector Cybersecurity Operations Centre capable of receiving, triaging, and escalating the report.

This is the hinge of the argument developed in Part IV of this paper, namely that resilience outcomes across Kenya's designated sectors track the presence or absence of this sectoral tier rather than any difference in the legal obligations owed. Where a sector regulator has the resources and the leverage to build the required center, the regime functions. Where it does not, the

24-hour reporting duty has no addressee, the sectoral tier of the audit and escalation chain is missing, and the designated owner is left, in practical terms, subject only to the general and untestable standard in section 41 of the DPA.

C. Constitutional Limits on Expanding the Framework

None of this means the framework has developed without cost, and the recent constitutional history matters for what can realistically be recommended.

On 15 October 2025, the President of the Republic of Kenya assented to the Computer Misuse and Cybercrimes (Amendment) Act, 2025 (Act No. 17 of 2025) (CMCA Amendment), which commenced on 4 November 2025. The amendment addressed genuinely new threats, broadening the phishing offense in section 30 to cover deceptive emails and telephone calls. It also expanded the state's reach considerably: it enlarged the cyber harassment offense in section 27 to cover communication likely to cause a person to commit suicide, and inserted a power in section 6(1)(j)(a) enabling the Committee to direct internet service providers to render websites and applications inaccessible where they were suspected of hosting content linked to terrorism, violent extremism, or child sexual exploitation, without prior judicial authorization (Human Rights Watch, 2025; Vellum Kenya, 2025).

The courts responded to these amendments twice. On 22 October 2025, a week after assent, Mugambi J issued conservatory orders in proceedings brought by Reuben Kigame and the Kenya Human Rights Commission, suspending the enforcement of sections 27(1)(b), 27(1)(c) and 27(2) pending the hearing and determination of the petition (Citizen Digital, 2025). On 2 July 2026, in consolidated petitions brought by the Kenya Section of the International Commission of Jurists, ARTICLE 19 Eastern Africa, and the Bloggers Association of Kenya, Nyaundi J declared section 6(1)(j)(a) and section 27(1)(b) of the CMCA, as amended, unconstitutional and of no legal effect. Nyaundi J held that the

blocking power conferred sweeping censorship authority on an administrative body without adequate safeguards and that the suicide-inducement offense was impermissibly vague. The court declined to invalidate the amendments on privacy grounds, finding that the petitioners had not identified with sufficient precision how particular provisions infringed Article 31 (ICJ Kenya, 2026; The Star, 2026).

The pattern is instructive and is directly relevant to the reform proposals in Part VI of this paper. What the courts struck down was the coercive content-control expansion of the Committee's powers. What they left entirely undisturbed was the designation, audit, baseline security and incident reporting architecture examined above. Kenya's resilience framework is not constitutionally imperiled. The route to strengthening it that runs through audit, standards and sectoral supervision is available; the route that runs through administrative powers over speech and access is not.

Policy has moved in the same direction as the Regulations, though without adding to their force. The Draft National Cybersecurity Strategy 2025-2029 sets out pillars for incident response, emerging technology risk and minimum baseline standards, and calls for supply chain risk management and faster incident reporting to government nodes (Ministry of Interior and National Administration, 2025). As a strategy document rather than a binding instrument, it cannot compel action from any party. Its value lies in signaling where subsidiary regulation is likely to go next, and in that respect, it reinforces rather than replaces the 2024 Regulations.

Three propositions can now be stated with some confidence, and together they reframe the question this paper set out to answer.

First, Kenya does not lack a legal resilience standard. Since January 2022, the sectors named in Gazette Notice No. 1043 have carried critical information infrastructure designation, and

since February 2024 that designation has carried prescriptive, measurable and auditable obligations covering risk assessment, recovery objectives, disaster recovery sites, annual audit and rapid incident reporting. The obligations are as specific as any in the region.

Second, those obligations coexist with, rather than displace, the Data Protection Act. Regulations 31(1)(a)(ii) and 74 make the cumulative operation of the two instruments explicit. Any account of Kenya's resilience deficit that depends on organizations choosing one statute over the other is therefore untenable.

Third, and consequently, the deficit cannot be explained by the content of either statute considered on its own. It has to be explained by what has and has not been built underneath them. The 2024 Regulations depend on an institutional chain: a sector regulator that has stood up and funded a Sector Cybersecurity Operations Centre, a Director who has appointed auditors, an audit cycle that produces findings, and a Committee that acts on them. Where that chain exists, the obligations take effect. Where it does not, they remain text. Part IV of this paper examines four designated sectors in which that chain is present in one case and absent in three.

IV. FOUR DESIGNATED SECTORS, ONE FUNCTIONING CHAIN

A. Finance: What Implementation Looks Like

Banking and finance were designated as critical information infrastructure sectors by Gazette Notice No. 1043. In finance alone, the institutional chain contemplated by the 2024 Regulations has actually been assembled, and the sector consequently provides the clearest available evidence of what the framework does when it is operationalized.

The Central Bank of Kenya (CBK) had exercised supplementary cybersecurity oversight over regulated institutions well before the 2024 Regulations were made, through the Commer-

cial Banks Cybersecurity Guidelines 2017 and the Payment Service Providers Cybersecurity Guidelines 2019. On 22 September 2025, it announced the establishment of the Banking Sector Cybersecurity Operations Centre, describing it expressly as a key component in the implementation of the Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024 and as a strategic initiative under its Strategic Plan 2024-2027 (Central Bank of Kenya [CBK], 2025). The Centre sits within the Bank's Cyber Fusion Unit and provides cyber threat intelligence, incident response, digital forensics, and cyber investigations to the regulated financial sector. The CBK simultaneously announced that it had begun harmonizing its two existing sets of guidelines with the 2024 Regulations, and directed that, pending completion of the harmonization exercise, all regulated institutions must comply with both sets of requirements and report cybersecurity incidents to the Centre within the timelines specified in the Regulations (CBK, 2025).

Read against regulation 11, the significance of this is precise rather than merely encouraging. The Central Bank has not created a parallel regime. It has occupied the position that regulation 11(1)(a) assigns to it as the sector regulator, deeming it the Sector Cybersecurity Operations Centre, and it has absorbed the operating costs that regulation 11(4) places on the sector regulator. In doing so, it has supplied the missing addressee for the 24-hour reporting duty in regulation 65(c), and the intermediate escalation tier between individual designated owners and the national center.

Three further points follow. First, the trigger was evidently sectoral necessity rather than general legal obligation. The CBK's financial stability reporting for 2025 recorded that fraud cases in the banking sector more than doubled during 2024, from 153 to 353, with amounts exposed of approximately 1.9 billion Kenyan Shillings and actual losses of approximately 1.5 billion (Ecofin Agency, 2025). The general law had applied unchanged

throughout that deterioration without prompting the establishment of the Centre. What prompted it was the deterioration itself, together with the Central Bank's own supervisory interest in the stability of the institutions it licenses.

Second, the mechanism that gives the arrangement force is licensing leverage: the CBK can attach cybersecurity compliance to an institution's authorization to operate, which is a sharper instrument than an administrative fine and one that no general-purpose regulator possesses. This is the sense in which the Computer Misuse and Cybercrimes framework, for all its prescriptive detail, still required a sectoral push to become operative, as the framework supplies the standards while the sector regulator supplies the consequence for ignoring them.

Third, and importantly for the argument, the DPA applies to banks in precisely the same way and to precisely the same extent as it applies to hospitals, insurers and health payers. Banks are controllers, their customers are data subjects, and sections 41 and 43 of the DPA bind them. The general law is therefore constant across the sectors compared below, and it cannot be the variable that explains the difference in outcomes; any argument that treats it as such is unsound. The variable is the presence or absence of the sectoral tier.

However, a qualification is warranted. The Centre is recent, and its effectiveness cannot yet be assessed on outcomes. The Bank's own procurement record shows it subsequently sought consultancy support for the design of an implementation plan, operating model, and governance structures for the Centre and for an accompanying sectoral cybersecurity framework (CBK, 2026). What can be said is narrower but still significant: in one sector, the institutional preconditions for the 2024 Regulations to function now exist, and a regulated institution that fails to report an incident within the prescribed period now faces a supervisor with both the information and the leverage to respond.

B. Health: The Same Obligations Without the Institution

Health was designated by the same Gazette Notice, in the same year, on the same statutory basis. The obligations in the 2024 Regulations therefore apply to designated health systems on identical terms. The institutional chain, however, was never assembled.

The threat environment in the health sector is not in doubt, as the National KE-CIRT/CC recorded a 95% increase in ransomware incidents against the healthcare sector, rising from 20 to 39 cases in October 2024 alone (CA, 2025a). A ransomware attack on a hospital is not principally a privacy incident but an operational one, because it locks clinicians out of records they need to treat a patient in front of them.

The regulatory environment is unusually crowded. The Data Protection Act classifies health data as sensitive personal data, placing its handling under the oversight of the ODPC. The Digital Health Act, 2023 layers a second regime on top, establishing the Digital Health Agency and mandating an interoperable Health Information Exchange so that patient records can move between facilities, insurers, and government systems. The Agency's draft Digital Health (Data Exchange) Regulations, 2024 would add a requirement that any organization exchanging health data through the Exchange hold a separate enterprise user license, distinct from, and additional to, its obligations as a controller or processor (Ministry of Health, 2024).

What the health sector conspicuously lacks, despite this density of regulation, is the one institution the 2024 Regulations actually require: a funded Sector Cybersecurity Operations Centre standing in the position regulation 11(1) assigns to the sector regulator or relevant Ministry. Neither the Ministry of Health nor the Digital Health Agency has established one. The consequence is structural rather than rhetorical. The 24-hour incident reporting duty in regulation 65(c) has no operational recipient in health. The sectoral tier of the escalation chain in regulations 10

and 11 is absent. And the sector's regulators possess no equivalent of the Central Bank's licensing leverage over the full range of relevant actors, which include insurers, hospitals, and connective platforms.

The M-Tiba breach shows what that absence produces. On 28 October 2025, a group identifying itself as Kazu began advertising a dataset of approximately 2.15 terabytes, comprising some 17 million files, said to have been taken from M-Tiba, a mobile health wallet developed by CarePay in partnership with Safaricom and the PharmAccess Foundation and used by more than 4 million Kenyans to manage medical payments and insurance claims (TechCabal, 2025a; HapaKenya, 2025). A sample covering some 114,000 users included national identity numbers, dates of birth, insurer names and, in some records, clinical diagnoses and the names of treating doctors (Techweez, 2025). CarePay's internal status report, shared with insurers including Jubilee, Fidelity, GA Insurance and AAR Insurance, put the confirmed figure at approximately 4.8 million records and disclosed that the intrusion had run from 17 to 25 October 2025 and was discovered only on 27 October 2025 (TechCabal, 2025b).

Four features of the incident bear on the argument.

The intrusion vector was a connected third party; attackers compromised the device and credentials of a third-party healthcare provider connected to the platform and used them to reach M-Tiba's systems (TechCabal, 2025b). This is precisely the risk that regulation 13 of the 2024 Regulations addresses, requiring notification to the Committee before outsourcing, a written agreement, prior risk assessment where database access is granted, and quarterly reporting by the service provider, with the owner remaining responsible for outsourced capabilities. It is also the risk regulation 36 addresses in requiring that integration with third-party infrastructure satisfy safety standards evaluated by the Director. The obligations existed, yet there is no public record of their having been verified in respect of this platform.

The detection gap was ten days, as the 72-hour clock in section 43 of the Data Protection Act begins only when a controller becomes aware of a breach carrying a real risk of harm. A ten-day detection gap therefore starts that clock ten days after the compromise, with no statutory consequence attaching to the delay in detection itself. Regulation 31(2)(f) of the 2024 Regulations does address detection, requiring appropriate security monitoring and response processes for timely detection of incidents, and regulation 31(2)(i) requires periodic testing of continuity and recovery plans; again, the gap is not in the text.

The notification chain failed at both ends. CarePay is a processor; the affected records belong to multiple insurers and payers who hold the controller relationship with the patient. Staff at Jubilee and AAR reported learning of the incident from media coverage rather than from CarePay (TechCabal, 2025b). The ODPC stated on 29 October that it had become aware of the incident through media reports, and that it was engaging with the processor and other stakeholders to establish the facts (Streamlinefeed, 2025; TechCabal, 2025b). A statutory notification duty of which the regulator learns from the press has not been complied with in substance, whatever the position on the 72-hour clock.

The response came from the privacy regulator alone. The ODPC opened an investigation under the Data Protection Act. Health being a designated sector, an incident of this magnitude also engaged the Computer Misuse and Cybercrimes framework, but there is no public record of a corresponding process under it, and no Sector Cybersecurity Operations Centre existed to receive the 24-hour report that regulation 65(c) of the 2024 Regulations requires.

It should be acknowledged that the Office of the Data Protection Commissioner has not been passive in this sector. In March 2025, the Data Commissioner confirmed that the Social Health Authority, having conducted a data protection impact assessment, remained subject to a post-implementation audit,

exercising the section 23 power discussed in Part II of this paper (Siaya Today, 2025). Therefore, the point is not that the privacy regulator has been inactive; rather, it has been operating alone in a sector where statutory design contemplates a second supervisory tier that does not exist.

Interoperability was not the wrong policy; it has real public health value. However, it multiplies the number of parties whose security posture determines the resilience of the whole, and the instrument that requires that multiplication to be assessed in advance, the 2024 Regulations, has no institutional presence in the sector that is doing the multiplying.

C. E-Government: The Same Statutes, Divergent Outcomes

Kenya's e-government infrastructure demonstrates the same lesson from the state's own side of the ledger, and it does so under conditions that hold the applicable law constant: the platforms compared below were subject to identical statutory obligations, so any difference in outcome must be attributed to something other than the law.

In late July 2023 a distributed denial-of-service campaign attributed to the collective Anonymous Sudan disrupted the eCitizen portal, through which more than 5,000 government services were then delivered. The Cabinet Secretary responsible for information, communications and the digital economy confirmed the attack publicly on 27 July 2023, describing an attempt to overload the system with extraordinary requests and stating that no data had been lost (Kitili & Abiero, 2023). The disruption extended to entities integrated with the platform, including the Kenya Power and Lighting Company, Kenya Railways Corporation and the National Transport and Safety Authority, and to mobile money and digital banking transactions dependent on those integrations (Kitili & Abiero, 2023). The National KE-CIRT/CC recorded the episode in its own quarterly reporting, noting that although web application attacks were numerically modest that quarter their impact was significant, as the eCitizen

incident and the resulting unavailability of online public services demonstrated (CA, 2023).

On 17 November 2025, a group identifying itself as PCP@ Kenya defaced multiple government websites simultaneously, replacing them with white supremacist slogans. The affected platforms included the portal of the presidency and the websites of the ministries responsible for interior, health, education, energy, labor, and water, together with the Directorate of Criminal Investigations and several other government-affiliated platforms (The Record, 2025; Nation, 2025). The Government confirmed the incident the same day, attributed it to the named group, and reported that incident response and recovery procedures had been activated (State Department for Internal Security and National Administration, 2025).

What makes the November 2025 incident analytically useful is the divergence within it. A substantial group of government platforms was untouched by the same coordinated campaign: eCitizen, the National Transport and Safety Authority, the Judiciary, the Kenya National Examinations Council, and the National Police Service all remained operational, as did the systems of the Ministry of Defence and the National Treasury (Nation, 2025).

The inference to be drawn requires care, because the obvious one is wrong. Every system involved, on both sides of the divide, operated under the same Data Protection Act. Every system involved also operated under the same Computer Misuse and Cybercrimes Act, the same Gazette Notice No. 1043 and the same 2024 Regulations. Neither statute can explain the divergence, because neither statute varied across the systems compared. It follows that the difference cannot be attributed to a deficiency in the Data Protection Act, and any argument that so attributes it is unsound. It equally cannot be attributed to a deficiency in the drafting of the 2024 Regulations.

As of 17 November 2025 neither regime was operating as a differentiating constraint. Whatever separated the platforms

that stayed up from the ministry sites that did not, it was a difference in the maintenance and hardening of individual systems rather than in the obligations owed by them. Those obligations are addressed in terms by regulation 31(2)(h) of the 2024 Regulations, which requires infrastructure and cybersecurity measures to mitigate equipment failure including maintenance and software updates, and by regulation 34(3)(e), which addresses configuration review, secure configuration, hardening and patching before deployment. Both applied to the ministry sites. The difference between compliance and noncompliance produced no antecedent consequence, because no audit under regulations 44 to 50 had established the position and no supervisory tier had acted on it. There is a further point worth noting: eCitizen, which was the principal casualty of the 2023 campaign, was among the platforms unaffected in 2025. Where remediation has occurred in Kenyan e-government it appears to have followed a public failure rather than a regulatory finding, which is precisely the sequence a functioning audit regime exists to reverse.

The government's own infrastructure is thus the clearest possible demonstration that the resilience deficit is one of verification rather than of legislative content.

D. Telecommunications: Designated, Disrupted, Undocumented

Telecommunications sits in the first line of Gazette Notice No. 1043, and the designated systems named under that head include cellular network components, international internet gateways, broadband networks, internet exchange points and centrally hosted processing platforms (NC4, 2022). It is nonetheless the sector least examined through a resilience lens, largely because the disruptions it produces rarely look like the attacks that dominate the rest of this analysis.

The concentration risk is documented by the sector regulator. In the quarter from July to September 2025, mobile subscriptions reached 78.3 million, a penetration rate of 149.4%,

with Safaricom holding 65.3% of subscriptions; mobile money subscriptions reached 48.6 million, a penetration rate of 92.8% (CA, 2026b). Safaricom's M-Pesa accounted for approximately 89% of mobile money subscriptions in the following quarter (CA, 2026c). M-Pesa is not one financial product among several. It is the settlement rail on which utility billing, paybill merchants and a considerable share of bank-to-customer transfers depend, which is why an outage propagates well beyond Safaricom's own customer base, as it did when Kenya Power publicly directed customers to alternative channels during a January 2024 paybill outage (Connecting Africa, 2024).

That outage was the second in the same month, and the response to both followed a pattern that recurred through 2024 and 2025: a brief acknowledgment on social media, no technical explanation of root cause, and restoration within a few hours to a day (TechCabal, 2024). A more severe disruption followed in September 2025, when customers reported an outage lasting more than 12 hours affecting calls, data and M-Pesa simultaneously. The operator initially attributed it to a network fault before later confirming that it was mid-migration to a new core mobile money platform, Fintech 2.0, marketed as strengthening resilience and capacity (The Kenya Times, 2025a, 2025b). There is genuine irony in an outage caused by the process of upgrading resilience infrastructure, which is nonetheless, for the hours it lasts, a resilience failure.

These incidents are not privacy breaches, so section 43 of the Data Protection Act is not engaged. Nor, on the public record, are they attacks, so the offense provisions in Part III of the CMCA are not engaged either. But the resilience obligations in the 2024 Regulations do not depend on an incident being an attack. Regulation 17(3)(a) requires the identification of single points of failure that may cause disruption to critical activities. Regulation 17(4)(b) requires the business impact analysis to be based on recovery time objectives and maximum acceptable outage. Regulation 26(2) requires prior notification to the Direc-

tor before any significant change to the design, configuration, security, or operations of designated infrastructure, defined in regulation 26(1) as a new system, integration, or modification whose new functionalities may compromise the confidentiality, integrity, and availability of the critical service. A core platform migration on the country's dominant payment rail is, on any reasonable reading, such a change.

Whether that notification was given, and whether the Director evaluated the implications as regulation 26(4) requires, is not a matter of public record. That is the gap in this sector, and it is narrower than that in health. The obligations exist and the Communications Authority is the deemed Sector Cybersecurity Operations Centre under regulation 11(1)(a). What is missing is any public accounting comparable to what section 43 of the Data Protection Act produces for a personal data breach. A recurring 12-hour failure of the country's dominant payment rail arguably warrants a mandatory public account of the incident, published within a fixed period, of the same kind that section 43 of the DPA compels after a personal data breach. At present nothing requires one.

The evidence here is a pattern of recurring and publicly underexplained outages rather than a single well-documented breach, and the conclusion is correspondingly narrow. Extending the existing audit and disaster recovery requirements, already binding on this sector, to include a mandatory public disclosure obligation following any outage above a defined severity or duration threshold would close this specific gap without new primary legislation.

The comparison is unusually clean because the general law is held constant: all four sectors are designated under the same Gazette Notice, all four are subject to the same 2024 Regulations, and all four are subject to the Data Protection Act in identical terms. The only variable that moves across the four is whether a sector regulator has built and funded the supervisory tier the Regulations assume.

In finance, it has; in health, e-government and telecommunications, it has not, or not in a form that has produced any visible verification. The resilience outcomes track that variable rather than any feature of either statute, and this is the empirical basis for the claim advanced in Part I of this paper: the resilience deficit is overwhelmingly a problem of institutional construction and enforcement, with one narrow drafting gap of real but subordinate significance.

V. THE ENFORCEMENT ASYMMETRY AND ITS CAUSES

A. An Active Regulator, Active in One Direction

It would be inaccurate to describe the ODPC as inert. It maintains the register of data controllers and processors required by Part III of the DPA, has issued guidance and codes to operationalize the DPA, and has brought a number of enforcement actions to a public conclusion. In late September 2023 it issued penalty notices totaling 9,375,000 Kenyan Shillings against three organizations for unlawful processing, with individual penalties ranging from 1,850,000 to 4,550,000 Shillings (Clyde & Co, 2023). It has also exercised its audit power under section 23, confirming in March 2025 that the Social Health Authority remained subject to a post-implementation audit notwithstanding its completed impact assessment (Siaya Today, 2025).

The pattern in the enforcement record is nonetheless consistent. The concluded matters concern unlawful processing, disclosure without consent, or breach of the data protection principles. None concerns a resilience failure as such: an entity with inadequate backup arrangements, an untested incident response plan, or infrastructure that collapsed under attack. This is not because such failures are not occurring; the National KE-CIRT/CC's own incident reporting leaves no doubt that they are (CA, 2025a, 2025b). It is because the Data Protection Act gives the Commissioner very little to enforce on that front. A regulator in-

vestigating a resilience failure under section 41 of the DPA must argue that the measures in place were not 'appropriate,' which invites precisely the dispute that a 30-day localization deadline or an adverse audit finding does not.

There is also a ceiling on what enforcement can achieve where the Commissioner does act. Section 63 of the DPA provides that the maximum penalty that may be imposed in a penalty notice is up to 5 million shillings, or in the case of an undertaking up to 'one per centum of its annual turnover of the preceding financial year, whichever is lower.' That statutory formulation means that for any undertaking with turnover above 500 million shillings, roughly 3.9 million United States Dollars, the effective ceiling is a flat 5 million shillings regardless of the size of the entity or the seriousness of the failure. Measured against an incident on the scale of the M-Tiba breach, a maximum of 5 million shillings functions less as a deterrent than as a cost of doing business.

A pending Data Protection (Amendment) Bill, 2025 would reverse the formulation to whichever is higher, materially raising the ceiling for large organizations, and would establish a dedicated Data Protection Appeals Tribunal intended to resolve complaints within 60 days rather than through the High Court's general docket (Recording Law, 2026). That reform addresses the deterrence problem on the privacy side of the asymmetry. It does nothing about the supervisory gap in the critical infrastructure framework, and the two need to be tracked as complements rather than substitutes.

B. Fiscal Capacity Across a Multiagency Framework

The capacity constraint is real but it is not confined to the privacy regulator, and framing it as an ODPC problem misstates it. The Computer Misuse and Cybercrimes framework is deliberately multiagency. The Committee draws its membership from across government; the Communications Authority operates the national incident response center; regulation 11 of the 2024 Reg-

ulations makes every sector regulator a Sector Cybersecurity Operations Centre and regulation 11(4) makes each of them bear the cost; regulation 67 required the National Police Service to establish a cybercrimes desk with trained personnel at every police station and police post within 12 months of commencement.

That distribution of duties is also a distribution of unfunded mandates. The pattern in Part IV of this paper is explained better by differential fiscal and supervisory capacity across those agencies than by any single institution's shortcomings. The Central Bank is a well-resourced regulator with a direct supervisory interest in the stability of the institutions it licenses; it built its Centre. Sector regulators without comparable resources or leverage have not, and regulation 11(4) gives them no funding stream with which to do so.

Within that wider picture, the position of the privacy regulator is documented. Research by the Kenya Institute for Public Policy Research and Analysis found that the ODPC was allocated only 270 million Kenyan Shillings for the 2022/23 financial year, a sum materially lower than the budgets of comparable regulatory bodies within the same ministry, and that it had consequently been unable to build enforcement mechanisms for matters such as data localization even though both statutes contemplate them, concentrating its capacity instead on registration and public awareness (KIPPRA, 2024).

This is not a criticism of any regulator's leadership so much as an observation about institutional incentives under scarcity. A regulator allocating a constrained enforcement budget will rationally prioritize cases that are quick to investigate, cheap to prove and likely to produce a communicable public result. An unauthorized disclosure with a clear paper trail meets all three criteria. A resilience failure requires forensic capacity to establish what happened technically, a defensible standard against which to measure conduct, and a much longer investigation. The asymmetry in the enforcement record is the predictable output of a framework that supplies an easy standard to one under-re-

sourced institution and a hard one to a chain of institutions that have not been funded to enforce it.

The practical implication is that closing the resilience gap cannot be a matter of asking the ODPC to enforce harder within its existing tools and budget. Its tools are the wrong ones for the task, and its budget could not support the task even if they were. Any credible reform package must pair a Computer Misuse and Cybercrimes-based supervisory mechanism, which the Committee and sector regulators rather than the privacy regulator are statutorily positioned to run, with funding specific enough that it cannot be absorbed into general ministry spending.

VI. A SEQUENCED REFORM AGENDA

Recommendations in this field tend to list everything a country could conceivably do without asking which of them are achievable given the institutions, politics and priorities in play. What follows is sequenced by difficulty, from steps requiring no new legislation to those requiring sustained fiscal and political commitment.

A. Phase One: Administrative Coordination

The cheapest available reform is a memorandum of understanding between the ODPC and the Committee routing resilience-adjacent matters, reports of prolonged outages, ransomware incidents, and infrastructure failures affecting personal data, to the Committee for technical investigation under the CMCA, while the privacy regulator retains jurisdiction over the consequences for data subjects. Nothing in either statute prevents this division of labor today. The ODPC's Strategic Plan already signals an intent to work more closely with sectoral regulators (ODPC, 2024); what is missing is the instrument.

Second, the Committee should publish the register of designated critical information infrastructure that regulation 25 al-

ready requires the Director to keep and maintain, to the extent consistent with the exemptions in regulation 18(5). At present, a health payer, insurer or platform operator cannot readily establish whether it is a designated owner and therefore whether the obligations in regulations 17, 31, 42 and 65 apply to it; publication requires no amendment and would convert an existing obligation into a knowable one.

Third, the Committee should publish, as guidance rather than binding regulation, a model third-party risk assessment checklist for organizations connecting to shared data exchange infrastructure of the kind the Health Information Exchange creates. The M-Tiba breach entered through a connected third party's compromised credentials, and regulations 13 and 36 already impose duties in respect of outsourced capabilities and third-party integration. A published checklist would give platform operators and their regulators a shared reference for what due diligence on a connected party means, at the cost of the drafting effort.

B. Phase Two: Subsidiary Regulation and Sectoral Build-Out

The Cabinet Secretary has authority under section 71 of the Data Protection Act to make regulations giving further effect to the Act. That authority could be used to add a testing and evaluation requirement to section 41(4) of the DPA, modeled on Article 32(1)(d) of the General Data Protection Regulation, without parliamentary amendment of the primary Act. This is the change most directly responsive to the single genuine drafting gap identified in Part II of this paper. It would not name specific technical measures, preserving the flexibility the standard is designed to protect, but it would require organizations to demonstrate that whatever measures they chose had been tested within a defined period. Because it would bind all controllers rather than only designated owners, it is the reform that reaches the large majority of Kenyan organizations that fall outside the critical infrastructure regime entirely.

In parallel, the Data Commissioner should finalize the draft Data Protection (Conduct of Compliance Audit) Regulations, 2024, which have been the subject of public consultation and which would set out both the procedure for audits conducted by the ODPC and the accreditation of external auditors (DLA Piper, 2026). Publishing criteria governing the exercise of the section 23 power was urged by independent reviewers more than 6 years ago and remains outstanding (Defenders Coalition et al., 2020). An audit power without published criteria is difficult to plan for, easy to characterize as arbitrary, and correspondingly underused.

The most consequential Phase Two reform, however, lies on the Computer Misuse and Cybercrimes side. The Ministry of Health, as the relevant Ministry for the purposes of regulation 11(1)(b), should establish a Health Sector Cybersecurity Operations Centre. The Central Bank's Centre demonstrates that this can be done within the existing regulatory framework, without amendment, by a regulator that decides to occupy the position the Regulations already assign to it. Doing so would supply the missing recipient of the 24-hour incident reports from designated health systems and the intermediate escalation tier between platform operators and the national center. The draft Digital Health (Data Exchange) Regulations, 2024, still in draft, are the natural vehicle: they can import the audit, disaster recovery, and third-party assessment obligations of the 2024 Regulations directly into the Health Information Exchange framework and designate the Digital Health Agency's role in relation to the sectoral center. The drafting window is open now, which makes this a question of timing rather than of political difficulty.

Finally, the Communications Authority, already the deemed Sector Centre for telecommunications, should be required to publish post-incident technical accounts for outages above a defined severity or duration threshold affecting designated infrastructure. This can be achieved through the Authority's existing licensing conditions and the reporting architecture in regulations 14 and 65 and does not require primary legislation.

C. Phase Three: Legislative and Fiscal Commitments

The harder reforms are fiscal and legislative, and they should be pursued in that order.

A ring-fenced budget line for the ODPC, structurally protected from absorption into general information and communications technology ministry allocations, would address the capacity constraint the Kenya Institute for Public Policy Research and Analysis documented (KIPPRA, 2024). This will attract resistance from the National Treasury on ordinary fiscal-discipline grounds, since ring-fencing narrows the room to reallocate across a tight fiscal year, and recent finance legislation has generated substantial public and parliamentary friction over smaller allocation questions. Framing the request specifically as resilience infrastructure funding, analogous to the Central Bank's investment in its own Centre, rather than as a general budget increase, ties it to a demonstrable capability gap and is more likely to survive scrutiny.

The more important fiscal reform, and the one that follows directly from the analysis of fiscal capacity in Part V of this paper, concerns regulation 11(4). Placing the operating costs of every Sector Cybersecurity Operations Centre on the sector regulator, without any accompanying appropriation, guarantees that the regime will be implemented only by regulators that are independently well-resourced. If the Regulations are to operate across all designated sectors rather than one, that allocation needs either a funding mechanism or a levy on designated owners, on the model by which several Kenyan regulators are already financed by the industries they supervise.

The pending Data Protection (Amendment) Bill, 2025 should be tracked as a complement to these steps rather than a substitute for them. Raising the section 63 ceiling and creating a dedicated tribunal would strengthen the financial incentive to invest in compliance on the privacy side of the asymmetry, which is the sense in which deterrence is used here; the argument is not

that organizations are indifferent to breaches, but that a ceiling of five million shillings is too low to influence the investment decisions of a large undertaking. Neither reform addresses the supervisory gap.

Direct legislative amendment of the CMCA to give the Committee licensing-style leverage over designated owners, in the manner the Central Bank exercises over banks, is the most difficult reform and should be approached last and narrowly. The judgment of 2 July 2026 is instructive on how such an amendment would need to be drafted. What the High Court struck down was an administrative power over access to online content exercised without judicial authorization; what it left untouched was the audit and standards architecture (ICJ Kenya, 2026). An expansion of the Committee's authority framed as a power to condition continued operation of designated infrastructure on compliance with audit findings, subject to the procedural protections of the Fair Administrative Action Act and the appeal to the High Court that regulation 21(4) already provides, sits on the side of that line the courts have left open. An expansion framed in terms of control over communications does not.

VII. CONCLUSION

Kenya's digital economy has grown faster than the institutions meant to keep it standing, and the growth has been real enough that there is now a great deal worth protecting.

The argument advanced here has not been that the Data Protection Act (2019) is a poor statute. It operationalizes Article 31 of the Constitution competently, and the one criticism this paper makes of its text, the omission from section 41(4) of any duty to test and evaluate, is narrow and remediable by subsidiary regulation under an existing power. Nor has the argument been that responsibility for resilience should be moved from one statute to another. The DPA and the 2024 Regulations bind the same organizations simultaneously and are drafted to do so, as

regulations 31(1)(a)(ii) and 74 of those Regulations make explicit.

The argument has been that Kenya's resilience deficit has been persistently misdiagnosed as a gap in the law when it is a gap in institutional construction. Since January 2022, the sectors named in Gazette Notice No. 1043 have carried critical information infrastructure designation. Since February 2024, that designation has carried obligations as prescriptive as any in the region: annual risk assessment against defined recovery time objectives and maximum acceptable outage, disaster recovery sites in separate locations, annual audit by an appointed auditor with powers of entry and document production, prior notification of significant configuration change, and incident reporting within 24 hours. Almost none of this has been operationalized. The single exception, the banking sector, is also the single sector in which the outcomes look different, and it became an exception not because a different law applied to it but because a well-resourced regulator with licensing leverage decided in September 2025 to occupy the supervisory position the Regulations had assigned to it 18 months earlier.

The four sectors examined in this paper hold the general law constant and vary only the institution. Health, e-government and telecommunications are subject to the same statutes as banking, and in each the failures of the past three years have been failures of detection, patching, configuration control and disclosure, all of which the 2024 Regulations address in terms and none of which any regulator had verified. The government's own experience in November 2025 is the clearest case: systems on hardened infrastructure survived a campaign that took down systems on legacy hosting, and the two groups were governed by identical legal obligations throughout.

What follows for reform is more modest and more achievable than the usual prescription. Kenya does not need a new cybersecurity statute. It needs its sector regulators to occupy positions that subsidiary legislation has already assigned to them,

a funding mechanism that makes that possible for regulators without the Central Bank's balance sheet, a published register so that designated owners know they are designated, published audit criteria so that supervision is predictable, and one narrow amendment to section 41(4) of the DPA so that the general standard binding everyone else can be objectively enforced. Where the framework's most recent expansions have overreached, the courts have already marked the boundary, and they have marked it around powers over speech rather than around powers of audit and supervision.

Bridging Kenya's resilience gap will not be accomplished by asking the Data Protection Act to be something it is not. Nor will it be accomplished by drafting further obligations onto a framework whose existing obligations remain largely unverified. It will be accomplished by building the institutions those obligations already presuppose.

REFERENCES

Central Bank of Kenya. (2025, September 22). *Establishment of the Banking Sector Cyber Security Operations Centre (BS-SOC) [Press release].* https://www.centralbank.go.ke/uploads/press_releases/1217936769_Press%20Release%20-%20Establishment%20of%20Banking%20Sector%20Cyber%20Security%20Operations%20Centre.pdf

Central Bank of Kenya. (2026). *Request for proposal for the design and development of an implementation plan for a Banking Sector Cybersecurity Operations Centre (BS-SOC) and a comprehensive sectoral cybersecurity framework (Tender No. CBK/RFP/118/2025-2026).*

Citizen Digital. (2025, October 22). Court suspends cyber harassment section in new Computer Misuse law. https://www.citizen.digital/article/court-suspends-cyber-harassment-section-in-new-computer-misuse-law-n371763

Clyde & Co. (2023, October 6). *Data protection compliance in Kenya: ODPC issues penalty notices to three data controllers.* https://www.clydeco.com/en/insights/2023/10/data-protection-compliance-in-kenya-odpc

Clyde & Co. (2024, May 27). *Unlocking the potential of cybersecurity: Navigating the Computer Misuse and Cyber Crime Regulations 2024.* https://www.clydeco.com/en/insights/2024/05/unlocking-the-potential-of-cybersecurity-navigatin

Communications Authority of Kenya. (2023). *Cybersecurity report, first quarter 2023-2024 (July to September 2023). National KE-CIRT/CC.* https://www.ca.go.ke/sites/default/files/2023-10/Cybersecurity%20Report%20Q1%202023-2024.pdf

Communications Authority of Kenya. (2024). *Public notice: Use of licensed electronic certification service providers and dot KE domain names by designated critical information infrastructure.* https://www.ca.go.ke/public-notices

Communications Authority of Kenya. (2025a). *Cybersecurity report, second quarter 2024-2025 (October to December 2024). National KE-CIRT/CC.* https://ke-cirt.go.ke/wp-content/uploads/2025/01/2024-25-Q2-Cyber-Security-Report.pdf

Communications Authority of Kenya. (2025b). *Cybersecurity report, fourth quarter 2024-2025 (April to June 2025). National KE-CIRT/CC.* https://ke-cirt.go.ke

Communications Authority of Kenya. (2026a). *Cybersecurity report, first quarter 2025-2026 (July to September 2025). National KE-CIRT/CC.* https://ke-cirt.go.ke

Communications Authority of Kenya. (2026b). *Sector statistics report for the financial year 2025/2026, first quarter.* https://www.ca.go.ke

Communications Authority of Kenya. (2026c). *Sector statistics report for the financial year 2025/2026, second quarter.* https://www.ca.go.ke

Computer Misuse and Cybercrime (Critical Information Infrastructure and Cybercrime Management) Regulations, 2024, Legal Notice No. 44 of 2024 (Kenya). https://new.kenyalaw.org/akn/ke/act/ln/2024/44/eng@2024-02-16

Computer Misuse and Cybercrimes (Amendment) Act, 2025 (No. 17 of 2025) (Kenya). Kenya Gazette Supplement No. 170 (Acts No. 17).

Computer Misuse and Cybercrimes Act, 2018 (No. 5 of 2018, Cap. 79C) (Kenya). https://new.kenyalaw.org/akn/ke/act/2018/5/eng@2025-11-04

Connecting Africa. (2024, January). *Kenya Power redirects customers as M-Pesa suffers fresh outage*. https://www.connectingafrica.com

Constitution of Kenya, 2010.

Data Protection Act, 2019 (No. 24 of 2019, Cap. 411C) (Kenya). https://new.kenyalaw.org/akn/ke/act/2019/24/eng@2022-12-31

Defenders Coalition, Kenya Legal and Ethical Issues Network on HIV and AIDS, Muthuri, R., & Privacy International. (2020). *Analysis of Kenya's Data Protection Act, 2019. Privacy International*. https://privacyinternational.org/sites/default/files/2020-02/Analysis%20of%20Kenya%20Data%20Protection%20Act,%202019_Jan2020.pdf

Digital Health Act, 2023 (No. 15 of 2023) (Kenya).

DLA Piper. (2026). *Data protection laws of the world: Kenya*. https://www.dlapiperdataprotection.com/index.html?t=law&c=KE

Ecofin Agency. (2025, September 25). *Kenya launches cybersecurity operations center to protect banks*. https://www.ecofinagency.com/news-digital/2509-49001-kenya-launches-cybersecurity-operations-center-to-protect-banks

Faegre Drinker Biddle & Reath. (2020, October). *British Airways faces significantly reduced £20M fine for GDPR breach*. https://www.faegredrinker.com/en/insights/publications/2020/10/british-airways-faces-significantly-reduced-20m-fine-for-gdpr-breach

GSMA. (2024). *The mobile economy: Sub-Saharan Africa 2024*. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/

HapaKenya. (2025, October 28). *M-TIBA has been hacked and medical data of 4.8M people has been leaked*. https://hapakenya.com/2025/10/28/m-tiba-has-been-hacked-medical-data-of-4-8m-people-has-been-leaked/

Human Rights Watch. (2025, November 7). *Kenya: New cybercrime amendments threaten online expression*. https://www.hrw.org/news/2025/11/07/kenya-new-cybercrime-amendments-threaten-online-expression

International Commission of Jurists Kenya. (2026, July 2). *Court strikes down unconstitutional provisions of Kenya's Cybercrimes Amendment Act [Press release]*. https://icj-kenya.org/news/for-immediate-release-court-strikes-down-unconstitutional-provisions-ofkenyas-cybercrimes-amendment-act/

International Organization for Standardization. (2019). *Security and resil-*

ience: Business continuity management systems: Requirements (ISO 22301:2019).

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection: Information security management systems: Requirements (ISO/IEC 27001:2022).

Kenya ICT Action Network. (2024). Five years of Kenya's Data Protection Act. KICTANet.

Kenya Institute for Public Policy Research and Analysis. (2024). Strengthening data protection in Kenya: Opportunities and the way forward. https://kippra.or.ke/strengthening-data-protection-in-kenya-opportunities-and-the-way-forward/

Kitili, J., & Abiero, D. (2023, August 22). *Kenya's digital infrastructure under threat? A look at Anonymous Sudan's thwarted cyberattack attempt and its implications for Kenya's digital systems. Centre for Intellectual Property and Information Technology Law, Strathmore University.* https://cipit.strathmore.edu/kenyas-digital-infrastructure-under-threat-a-look-at-anonymous-sudans-thwarted-cyberattack-attempt-and-its-implications-for-kenyas-digital-systems/

Ministry of Health. (2024). *Digital Health (Data Exchange) Regulations, 2024 [Draft] (Kenya).*

Ministry of Interior and National Administration. (2022). National cybersecurity strategy 2022 (Kenya). https://ict.go.ke/sites/default/files/2024-09/Kenya%20Cybersecurity%20Strategy%202022.pdf

Ministry of Interior and National Administration. (2025). *Draft national cybersecurity strategy 2025-2029 (Kenya).*

Nation. (2025, November 17). Hackers target several government websites, temporarily take over presidency portal. https://nation.africa/kenya/news/hackers-target-several-government-websites-temporarily-take-over-presidency-portal-5267412

National Computer and Cybercrimes Co-ordination Committee. (2022). *Designation of critical infrastructure, Gazette Notice No. 1043, Kenya Gazette Vol. CXXIV, No. 21 (31 January 2022).*

National Institute of Standards and Technology. (2021). Developing cyber-resilient systems: A systems security engineering approach (NIST Special Publication 800-160, Vol. 2, Rev. 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-160v2r1

Office of the Data Protection Commissioner [ODPC]. (2024). *Strategic plan (Kenya).*

Recording Law. (2026). Kenya data privacy laws: DPA 2019, ODPC enforcement, and 2026 compliance guide. https://www.recordinglaw.com/world-laws/world-data-privacy-laws/kenya-data-privacy-laws/

Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1.

Ropes & Gray. (2020, October 16). *British Airways fined £20 million by ICO for data breach.* https://www.ropesdataphiles.com/2020/10/british-airways-fined-20-million-by-ico-for-data-breach/

Siaya Today. (2025, October 30). *ODPC probes alleged M-Tiba data breach as fears mount over health information exposure.* https://siayatoday.com/2025/10/30/odpc-probes-alleged-m-tiba-data-breach-as-fears-mount-over-health-information-exposure/

State Department for Internal Security and National Administration. (2025, November 17). *Statement on the cybersecurity incident affecting government websites (Kenya).*

Streamlinefeed. (2025, October 29). Kenya probes alleged M-Tiba leak of 4.8m health records. https://streamlinefeed.co.ke/news/kenya-probes-alleged-m-tiba-leak-of-48m-health-records

TechCabal. (2024). *Safaricom's M-Pesa suffers second outage this month.* https://techcabal.com

TechCabal. (2025a, October 28). *Safaricom-backed M-Tiba hacked, exposing patient records.* https://techcabal.com/2025/10/28/safaricom-backed-m-tiba-hacked-exposing-4-8-patient-records/

TechCabal. (2025b, November 12). *M-Tiba took 10 days to detect breach exposing 5m Kenyans' health records.* https://techcabal.com/2025/11/12/m-tiba-took-10-days-detect-breach-exposed-kenyan-health-data/

Techweez. (2025, October 28). *M-Tiba hack: Kenyan health data exposed.* https://techweez.com

The Kenya Times. (2025a). *Safaricom network outage disrupts calls, data and M-Pesa nationwide.* https://thekenyatimes.com

The Kenya Times. (2025b). *Safaricom confirms outage linked to Fintech 2.0 migration.* https://thekenyatimes.com

The Record. (2025, November 17). *Kenyan government websites back online after hackers deface pages with white supremacist messages. Recorded Future News.* https://therecord.media/kenyan-gov-websites-back-hack

The Star. (2026, July 2). *High Court strikes down State website-blocking powers in Cybercrimes Act.* https://www.the-star.co.ke/news/2026-07-02-court-strikes-down-state-powers-to-block-websites

Vellum Kenya. (2025, October). *Understanding the Computer Misuse and Cybercrimes (Amendment) Act, 2025.* https://vellum.co.ke/understanding-the-computer-misuse-and-cybercrimes-amendment-act-2025/

World Bank. (2023). *Kenya Digital Economy Acceleration Project.* https://www.worldbank.org

JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 6, Issue 1 (2026) p.101-168
https:doi.org/10.52907/jipit.2026.611

Who Owns the Face? Reimagining Image Rights in Kenya Through African Personhood

*Renee Tikolo**

ABSTRACT

The commercial circulation of African images through global digital platforms reveals how African identities are treated in global digital markets; extracted from their social and historical contexts, reduced to licensable assets, and monetized by foreign platforms while those depicted retain no control and receive no share of the proceeds. These images carry personal, historical, and cultural significance, yet current legal frameworks reduce them to mere intellectual property or personal data, borrowing Western categories that overlook the relational, historical, and personal meaning embedded in an individual's image. While dignity, memory, and social embeddedness are universally significant dimensions of human identity, African philosophical traditions offer a distinct and underutilized lens through which these values can be translated into a legally coherent framework for image rights, one that existing Western legal categories have failed to provide. This paper argues for reimagining image rights through a framework grounded in African conceptions of personhood, addresses both the conceptual inadequacy of existing legal categories and resists the extractive logic of data colonialism, recognizing individuals as both autonomous and relationally embedded. Drawing on the blended personhood model and the concept of data colonialism and combining doctrinal analysis of Kenya's legal framework with comparative examination of the European Union, France, and South Africa, the author proposes reforms operating at three levels: national, continental, and international, to ensure proper attribution, fair benefit-sharing, and cross-border accountability. At stake is more than ownership; it is the power to determine how African stories are represented, circulated, and valued, ensuring that dignity and identity are not erased behind a watermark.

* Renee Tikolo (LLB, PgD) is an Advocate of the High Court of Kenya, Teaching Assistant at Strathmore University Law School, and Researcher at Privacy Hub Africa. She is a member of the Association of Privacy Lawyers in Africa (APLA) and the Law Society of African AI Professionals (LSAAP). Her work examines how legal frameworks respond to digital transformation, with particular focus on data protection, digital governance, and AI regulation in African contexts.

Keywords: Image Rights, African Personhood, Relational Embeddedness, Digital Images, Data Colonialism

TABLE OF CONTENTS

ABSTRACT 101
I. INTRODUCTION 103
II. ANALYTICAL AND CONCEPTUAL FOUNDATIONS 110
A. *Image Rights within Western Frameworks* 110
B. *Communitarianism without Individuality* 111
C. *The Blended Model of Personhood Theory and the Re-Opening of Individuality* 113
D. *Counterarguments to the Blended Model of Personhood Theory* 116
III. KENYA'S LEGAL APPROACH TO IMAGE RIGHTS 119
A. *Constitutional Protection* 120
B. *Statutory Protection and its Limitations: The Data Protection Act and the Copyright Act* 122
C. *Judicial Interpretation of Image Rights in Kenya* 125
D. *Towards an African-Centered Approach to Image Rights* 126
IV. COMPARATIVE ANALYSIS OF IMAGE RIGHTS 128
A. *Image Rights in the European Union* 129
B. *Image Rights in France* 131
C. *Image Rights in South Africa* 134
D. *Key Insights from the Comparative Jurisdictions* 137
V. DATA COLONIALISM AND AFRICAN IMAGES 138
A. *Extracting and Commercializing African Images* 140
B. *Impact on the Narrative Control, Dignity and Identity of African Image Subjects* 143
C. *Kenya in the Global Landscape and Pathways for Reclaiming Control* 145
VI. RECOMMENDATIONS 149
A. *Integrating African Personhood into Kenyan Law* 151
B. *Reconceptualizing Image Ownership* 156
C. *Strengthening Continental and International Frameworks for Image Rights Protection* 159
VII. CONCLUSION 163

I. INTRODUCTION

In 2023, while exploring online archives for images documenting Kenya's cricketing history, I stumbled upon something both familiar and unsettling: photographs of my father, Steve Tikolo, one of Kenya's most recognizable sports figures, were being offered for licensing on commercial stock platforms such as Getty Images and Alamy, with each image carrying a price ranging from 19 to 499 US Dollars. At first, this appeared to be a routine matter of digital commerce. Yet the deeper I looked, the more concerning it became. For our family, these images are far more than visual artifacts. They are fragments of memory, marking personal milestones and moments of family significance. They are further woven into the fabric of national history, marking milestones in Kenya's sporting achievements, symbols of national pride, and Kenya's cricketing legacy.

The Maasai people of Kenya and Tanzania further illustrate this pattern with particular clarity: over 1,000 companies worldwide; among them Louis Vuitton, Calvin Klein, Ralph Lauren, and Jaguar Land Rover, have used Maasai imagery, iconography, and cultural identity in commercial campaigns and product lines without consent or any payment to those depicted (Brindle & Layton, 2017; Brindle & Florman, 2021), while approximately 80% of the Maasai population lives below the poverty line (Brindle & Florman, 2021). The harm here is not reducible to economics: the Maasai image is inseparable from the cultural identity of the individuals depicted, embodying lineage, ceremony, age-grade systems, and social belonging, dimensions wholly invisible to the transactional logic of global commerce (Hodgson, 2011). When such images are extracted from their social context and circulated as commodities, what is lost is not merely a revenue stream, but the authority of the individuals depicted and those connected to them, over how they are seen, remembered, and represented in the world.

Despite their deep personal and historical significance, these photographs circulate in the global market merely as commodi-

ties, but this experience is not isolated. Across Kenya and Africa, images of athletes, cultural figures and ceremonies, ordinary citizens and everyday life are scraped, indexed, and monetized by digital intermediaries operating far from the social, historical, and narrative contexts in which those images were created[1] (Couldry & Mejias, 2019; Milan & Treré, 2019; Birhane, 2023). Photographers and international agencies profit from licensing them, while those depicted, the persons themselves, their families, and their communities, have virtually no say in their use (Birhane, 2023). There is no visibility into how proceeds are distributed, no mechanism to ensure the images are handled with respect, and minimal opportunity to protect the dignity or legacy of those represented (Birhane, 2023; Ijuo, 2025). Each photograph, in this sense, becomes disentangled from the stories, relationships, heritage, and social context it embodies, circulating freely in markets and platforms far removed from the realities of Kenyan life and African memory (Birhane, 2023; Couldry & Mejias, 2019; Milan & Treré, 2019).

This practice is part of a broader pattern of digital extraction which Couldry and Mejias (2019) describe as 'data colonialism'. Data colonialism occurs when information about the Global South is appropriated, repurposed, and commercialized under Western frameworks of ownership and value (Couldry & Mejias, 2019, p.1). The issue extends beyond economics; it is ontological, and it raises a fundamental question: who truly owns African images, and according to what conception of ownership should that question be answered?

[1] Case law across the continent and multiple jurisdictions demonstrate this pattern of extraction. In Nigeria, the Court of Appeal in Banire v NTA-Star TV Network Ltd confirmed that copyright vests in the photographer, meaning images can be commercially exploited without the subject's knowledge or consent, leaving subjects entirely without recourse (Nwokedi, 2021). In Tanzania, the High Court in MultiChoice (T) Ltd v Three Elite Athletes (Civil Case No. 15 of 2021) [2023] found that images were used commercially without consent, exposing subjects to extraction by commercial entities. In Uganda, courts have similarly adjudicated cases where individuals' images were commercially exploited without permission (Bowmans, 2018).

The extraction of African images does not occur by accident, but follows a well-established and largely opaque commercial infrastructure. Getty Images illustrates this model with particular clarity, and while a fuller examination of platform infrastructure is examined in greater detail later in this paper, its essential features are as follows. Photographers upload or submit images to the platform, which then assumes the exclusive worldwide right to license that content and determine its pricing unilaterally, in return for a royalty paid to the contributor (Getty Images Contributor Agreement v5.1, n.d.). The person depicted in the image is entirely absent from this transaction (Getty Images Contributor Agreement v5.1, n.d.). This absence is not an oversight; it is built into the platform's legal architecture, which governs the relationship between contributor and platform exclusively, with no role, right, or remedy afforded to the subject of the image (Getty Images Contributor Agreement v5.1, n.d.; Getty Images, 2024b).

The structural mechanism that makes this possible is the editorial use classification (Getty Images, 2024b). Images depicting real people at news, sports, or cultural events are categorized as editorial content and do not require model or property releases, meaning the subject has given no consent to the licensing and has no contractual standing to object, to withhold permission, or to share in the proceeds (Getty Images, 2024b). As a result, a photograph of a Kenyan athlete can be submitted to a platform, priced at hundreds of dollars per license (Getty Images, 2024c), and sold to buyers across the world, with value flowing entirely among the photographer, the platform, and the purchaser, while the subject remains legally invisible to the transaction (Getty Images Contributor Agreement v5.1, n.d.; Getty Images, 2024b). It is within this global context of structural exclusion that Kenya's domestic legal framework must be assessed.

Kenya's legal framework offers a response to this reality, but it is a fragmented one. The Constitution recognizes dignity (Article 28), privacy (Article 31), and property (Article 40); provisions that are intentionally broad, creating space for courts to develop

image rights doctrine through purposive interpretation. However, judicial engagement with these provisions has remained sporadic and fragmented, falling short of a coherent framework adequate to the challenges posed by global digital image markets. At the statutory level, two instruments engage with image rights from fundamentally different angles. The Data Protection Act (DPA), 2019, approaches the image from the subject's perspective, classifying photographs as personal data (Section 2) and affording the depicted individual certain rights, including the right to consent to processing, to access their data, and to object to its use (Section 25). The Copyright Act, 2001, by contrast, approaches the image from the creator's perspective, protecting the photographer's moral and economic rights in the image as a creative work (Section 32), with no equivalent recognition of the subject's interests.

Together, however, these frameworks leave a distinct and critical category of interests unaddressed: the subject's interest in economic participation in the commercial use of their own likeness, in narrative authority over how they are represented and circulated, and in the protection of dignity understood not merely as an individual right but as reflecting the individual's relational identity, historical significance, and personal embeddedness, the dimensions of personhood that sit at the heart of this paper's argument. As a result, when images are commercialized without consent, individuals must navigate a legal landscape in which statutory provisions and constitutional principles operate largely in parallel rather than in concert, offering procedural remedies that do not reach the deeper harms at stake.

Courts have, on occasion, drawn on these constitutional principles to protect privacy, dignity, and personality (*Ann Njoki Kumena v KTDA Agency Ltd*, 2019; *Jessica Clarise Wanjiru v Davinci Aesthetics*, 2017; *Wanjiru v Machakos University,* 2022). However, no coherent doctrine on image rights has emerged from this case-by-case approach. The absence of such a framework leaves citizens exposed to global markets that treat African

images as extractable commodities (Couldry & Mejias, 2019). The consequence entrenches unequal power dynamics and denies recognition to the personal, historical, and relational significance these images carry for the individuals depicted (Milan & Treré, 2019; Birhane, 2023).

This global commodification of African images further perpetuates historical hierarchies (Milan & Treré, 2019; Birhane, 2023), privileging Western systems of authorship and ownership, which treat an image either as property owned by the creator or as a data point governed by consent rules, positioning the individual as an isolated rights-holder, while sidelining African understandings of personhood as both autonomous and relationally embedded (Honoré, 1961; Mamdani, 1996; Kahaka & Maundeni, 2022; Menkiti, 1984). The conceptual foundations of this alternative understanding are developed in Part II of this paper.

Viewed through this lens, image rights take on a deeper significance: a person's image is not merely an instrument of personal autonomy, nor simply property for commercial exploitation, but a space where individual identity and relational belonging converge, a carrier of personal history, narrative, and reputation. When an image of a Kenyan athlete or citizen is removed from its historical and social context and sold on a foreign platform, the harm to the individual is both personal and legally cognizable. At the level of dignity, the individual's intrinsic worth is undermined when their image is reduced to a generic commercial asset, a harm Kenyan courts have recognized as actionable (T.O.S. v Maseno University, 2016; Ann Njoki Kumena v KTDA Agency Ltd, 2019). At the level of privacy, the individual's right to control how their personal attributes are accessed is violated when their image is commercially exploited without consent (Jessica Clarise Wanjiru v Davinci Aesthetics, 2017). At the level of narrative authority, the individual loses control over how they are represented and remembered, an interest existing frameworks do not yet recognize but that this paper's proposed framework would give legal expression to (Kahaka & Maundeni,

2022; Menkiti, 1984). It is precisely because existing frameworks address only the first two dimensions while leaving the third unrecognized that this paper's proposed framework is necessary.

This paper therefore asks: How can Kenya develop a coherent image rights framework, one that, by grounding itself in African conceptions of personhood, addresses the conceptual inadequacy of existing legal categories and provides meaningful protection against the extractive practices of data colonialism? It further argues that the solution does not require a new legal regime but rather the reinterpretation and integration of existing laws through an African philosophical lens.

Specifically, this paper advances three claims. First, doctrinally, Kenya must bridge its fragmented protections by coherently operationalizing the already-recognized overlap between rights to dignity, privacy, and property in the specific context of image rights. This requires coordinated statutory interpretation and, where necessary, legislative refinement to clarify that individuals possess enforceable interests in their likeness beyond the economic rights of creators. Second, normatively, reform must be guided by African conceptions of personhood and dignity. In a blended-personhood framework, individuals are recognized as autonomous yet inherently connected to their communities (Kahaka & Maundeni, 2022). Translating this to image rights implies that harm occurs not only when consent is violated but also when the individual's relational identity, historical significance, and personal embeddedness are commodified without regard for their meaning to the individual depicted.

Finally, any reform must also navigate global power dynamics. Platforms such as Getty Images, Alamy, and Shutterstock profit from African images while remaining insulated from local law. Addressing this requires regional and international coordination, for instance through the African Union Data Policy Framework (2022) or the African Union Convention on Cybersecurity and Personal Data Protection, alongside national statutory reform. Such coordination should ensure that African norms

of dignity and relational personhood inform the application of these reforms across borders.

By framing the issue this way, this paper contributes to three scholarly conversations: it enriches African legal scholarship on personality and image rights, engages comparative perspectives from jurisdictions such as South Africa and France, and situates these debates within broader reflections on data colonialism, narrative authority, and recognition of local perspectives. It seeks to show that legal reform can do more than regulate markets: it can assert African norms of dignity, identity, and relational personhood as guiding principles for law in the digital era.

Methodologically, the author combines doctrinal analysis of constitutional and statutory provisions with targeted comparative study of foreign legal systems. The analysis is complemented by theoretical engagement with African communitarian philosophy and scholarship on data colonialism, creating a proposal for legal reform that is both practically enforceable and normatively grounded.

Part II of this paper lays out the conceptual foundations of image rights, distinguishing them from privacy, data protection, and copyright while introducing the African philosophical principles that guide this analysis. Part III maps Kenya's existing legal landscape, highlighting doctrinal gaps that allow image exploitation to persist. Part IV draws comparative lessons from selected foreign jurisdictions. Part V examines the role of digital infrastructures and data colonialism in shaping the global circulation and extraction of African images, and Part VI proposes an integrated framework for Kenyan image rights, informed by African conceptions of personhood and relational identity. The conclusion in Part VII draws together these threads to highlight the normative and practical significance of establishing an African-rooted legal framework for image rights, underscoring the importance of first clarifying the conceptual foundations of image rights before examining their legal and practical implications.

II. ANALYTICAL AND CONCEPTUAL FOUNDATIONS

The argument for developing an African-rooted legal framework for image rights must begin with an examination of the conceptual framework in which these rights sit. Before turning to the African philosophical foundations that underpin this paper, it is necessary to briefly situate image rights within the broader landscape of legal rights that protect or regulate the use of a person's identity, and to clarify why the inherited Western conceptual frameworks cannot adequately address the issues at stake for African subjects. Only after laying out this terrain does the African individual-communitarian blended model of personhood become visible as a coherent and normatively compelling foundation for regulating the circulation, appropriation, and commercialization of African images.

A. Image Rights within Western Frameworks

In most Western jurisdictions, the protection of an individual's image is historically distributed across several fields of law such as privacy, data protection, copyright, and publicity, each of which protects different interests. Privacy law focuses on shielding individuals from unwanted intrusion or disclosure (Warren & Brandeis, 1890), while data protection law, particularly within the General Data Protection Regulation (GDPR) framework, protects personal data, including biometric identifiers used to recognize a person (Regulation (EU) 2016/679; Voigt & Von dem Bussche, 2024). Furthermore, copyright law protects the rights of creators of images (in this case, photographers), not the subjects depicted (Ginsburg, 2016), and publicity rights, emerging predominantly in American jurisprudence, protect the commercial value of one's name, image, or likeness and prevent unauthorized commercial exploitation, with the right to privacy being inferred from U.S. constitutional principles and recognized in landmark cases (*Meyer v. Nebraska*, 1923; *Pierce v. Society of Sisters,* 1925). Each of these regimes frames the individual as

the central rights-bearing unit, and the law protects the image because it belongs to a rights-holding, autonomous subject whose economic or privacy interests deserve respect.

This legal architecture is undergirded by philosophical assumptions about personhood that are distinctly individualistic, providing that an individual is fundamentally self-possessing, autonomous, and prior to the community (Dwivedi, 2024, para.1). Thus, an image, as an extension of the person, is treated as something that derives from the individual and is owned or controlled by that individual. This is a view reflected in Western image rights doctrine, which protects the individual's dignitary and economic interests in their likeness (Synodinou, 2014). While this framework is internally coherent within Western liberal philosophy, it carries implicit assumptions that do not translate seamlessly into many African contexts. Crucially, it assumes that the meaning and value of an image derive primarily from the individual subject, rather than from the social relationships in which they are embedded.

This philosophical foundation, rather than doctrinal differences, creates a conceptual mismatch when Western frameworks are applied in African contexts. A model that presumes a self-standing individual cannot fully grasp how Africans and African communities understand identity, dignity, and representation. Therefore, a purely Western framing of image rights is analytically insufficient for this paper's central argument. To address this gap, it is necessary to examine African philosophical accounts of personhood, which offer alternative ways of understanding the individual, the community, and the interplay between personal and collective identity.

B. Communitarianism without Individuality

Within African philosophical literature, influential thinkers such as Mbiti (1969) and Menkiti (1984) have commonly been associated with a classical communitarian account of personhood. According to them, personhood is neither inherent nor automat-

ic; it is something achieved through active participation, incorporation and rootedness in the community (Mbiti, 1969; Menkiti, 1984). Thus, an individual becomes a 'full person' only by fulfilling social, moral, and cultural obligations within the community (Menkiti, 1984, p. 173). Menkiti (1984) famously argued that 'it is the community which defines the person, not some isolated static quality of rationality, will, or memory' (p. 172). In this formulation, the community is not merely a context for personhood, it is the source of personhood.

This interpretation has often been taken to imply that individuality, autonomy, and personal agency have little conceptual space within African thought, and because the community is the primary bearer of value, the individual is understood in terms of social embeddedness rather than self-possession. Mbiti's well-known formulation 'I am because we are, and since we are, therefore I am' reinforces this view by expressing the idea that existence itself is relational (Mbiti, 1969, p.106; Menkiti, 1984, p.171). The individual, on this account, does not stand apart from the collective; their identity is conferred and sustained by the social whole.

As a result, much of the comparative philosophical literature draws a sharp dichotomy; Western thought is cast as individualistic, prioritizing rights, autonomy, and self-possession, while African thought is cast as communitarian, prioritizing duties, social cohesion, and moral interdependence. Wilkinson (2002), discussing cultural differences in South Africa, suggested that Western notions of selfhood are simply inapplicable to African contexts because the African subject is primarily a 'being-in-relation', with identity derived externally rather than internally (Wilkinson, 2002). This rigid dichotomy has influenced legal theory, where frameworks built on assumptions of individualized identity may inadequately account for African subjects, whose sense of self is understood primarily through relational and communal ties.

What is important for this paper is not whether the classical communitarian interpretation is entirely accurate, it is increasingly challenged, but that it represents the dominant starting point in the literature. This framing is conceptually significant because image rights hinge on questions of identity, dignity, and individual interest. By portraying African personhood as incompatible with individuality, it creates an apparent obstacle to grounding a rights-based model in African thought. Recognizing this tension, however, sets the stage for the blended perspective developed in the following subsection, which demonstrates that African philosophical frameworks can simultaneously accommodate relational embeddedness and individual agency, providing a coherent foundation for African-rooted image rights.

C. The Blended Model of Personhood Theory and the Re-Opening of Individuality

Recent African authors have challenged the oversimplified dichotomy between an individualistic West and a communitarian Africa. Makotoka Kahaka and Wazha Maundeni (2022) argue that this binary misrepresents African thought, overlooking the ways in which African philosophy accommodates both communal and individual aspects of personhood. They propose a blended model of personhood: one that recognizes the centrality of the community while acknowledging that individuals retain agency, autonomy, and personal identity within that relational fabric (Kahaka & Maundeni, 2022).

Kahaka and Maundeni (2022) argue that individuals in African societies do not exist exclusively as communal beings nor exclusively as autonomous selves. Instead, they move between these two modes at different phases of life and in different contexts. For instance, they point out that rituals of initiation, communal obligations, and shared cultural responsibilities emphasize relational identity, while personal decision-making, individual achievements, and moral accountability reflect ele-

ments of individuality (Kahaka & Maundeni, 2022). In their formulation, 'there is a sense in which one and the same person can assume a communal and individualistic existence consecutively throughout his or her life' (Kahaka & Maundeni, 2022, p. 58). This insight is crucial because it disrupts the assumption that African thought is inherently incompatible with individual interests.

Kahaka & Maundeni's work demonstrates that African communitarianism is not collectivism as it does not erase the individual or absorb them into the group. Instead, it frames the individual as constitutively relational, but still capable of independent action and personal identity. In other words, individuality in Africa is not denied; it is contextualized. This repositioning is essential for developing an African approach to image rights because image rights depend on the recognition of personal identity, personal dignity, and personal harm. If African philosophy can support a model in which the individual is both embedded and autonomous, then image rights can be grounded in African thought without importing Western assumptions wholesale.

Furthermore, Kahaka and Maundeni's blended model provides a conceptual bridge that allows African normative frameworks to engage global debates on identity and representation without abandoning indigenous philosophical foundations. It becomes possible to argue that African subjects have personal claims over their images - not as isolated individuals in the Western sense, but as relational individuals whose identities are shaped by, and contribute to, their families, communities and the society. This shift opens space for legal recognition of personal control over images while remaining faithful to African ontologies.

The blended perspective does not stand alone; it is reinforced by other African scholars who insist that African communitarianism has always contained conceptual room for individual dignity and uniqueness. Amodu, Salisu Ameh, and Fatima Mohammed (2022) challenge the portrayal of African thought

as purely communal and argue that individuality has always been present, even if not foregrounded in earlier philosophical accounts. They emphasize that African societies historically recognized each person as both unique and socially embedded; that the community affirms existence and identity, but it does not extinguish personal worth. Their argument is captured powerfully in their observation that:

> 'the African notion of community is more germane than that of Rousseau or Hegel in that while emphasizing the corporate nature of human existence, it does not by that token deny individual liberty or the idea of every human being as both unique and important'. (Amodu & Mohammed, 2022, p. 102).

This reinforcement deepens the philosophical foundation necessary for this paper in two respects. First, African thought has its own internal resources for recognizing personal dignity and it does not require borrowing Western individualism to do so. Second, the uniqueness of individuals matters within African communities. A person participates in the community, but they also carry personal identity, personal agency, and personal worth, a worth expressed both through their relational embeddedness and their individual identity (Amodu & Mohammed, 2022). This is particularly significant for image rights because images do not merely depict biological individuals, they reflect personal identity, social belonging, and cultural meaning simultaneously. A philosophical model that recognizes individual worth as expressed through relational embeddedness therefore provides a stronger and more complete foundation for legal protection than Western individualism alone, one that aligns with the realities of how African images circulate and are appropriated globally and enables the law to respond to the fuller depth of harm to the individual that existing frameworks cannot currently see or remedy.

D. Counterarguments to the Blended Model of Personhood Theory

Before adopting the blended model as this paper's normative foundation, two significant counterarguments must be acknowledged and addressed.

First, African philosophical traditions are not uniform. Bayuo (2025) shows through the divergences between thinkers such as Mbiti, Menkiti, Gyekye, and Wiredu. The communitarian and blended conceptions of personhood discussed in this section draw primarily from subSaharan African philosophical literature, particularly the work of these scholars (Bayuo, 2025), and while they reflect widely shared values across many African communities, they do not capture the full diversity of philosophical traditions across the continent. Even within a single tradition, significant internal debates exist. For instance, among the Akan people of West Africa, Wiredu (1992, as cited in Bayuo, 2025) holds that personhood is graduated and socially acquired, while Gyekye (1995, as cited in Bayuo, 2025) argues that it is an essentially human capacity for reason, not social characteristics, that constitutes the basis for moral worth.

As Bayuo (2025) demonstrates, divergences exist even among the most prominent African philosophers of personhood. Mbiti and Menkiti emphasize earned personhood through communal participation, while Gyekye recognizes an inherent baseline of moral worth prior to community membership, and Wiredu argues instead that personhood is socially conferred through communal recognition (p. 5-6). Different communities across Africa hold different conceptions of identity, belonging, and the relationship between the individual and the collective, shaped by distinct histories, religions, languages, and social structures (Kahaka & Maundeni, 2022; Bayuo, 2025). The blended model is therefore not presented as a universal African truth applicable to every community and context. Rather, as Kahaka and Maundeni (2022) note, moderate communitarianism reflects a common feature within the diversity of different African communities, accommodating both communal values and values of individuality,

both ancient wisdom and current thinking, making it a widely grounded rather than narrowly prescriptive philosophical framework (Kahaka & Maundeni, 2022, p. 58).

Second, post-colonial shifts in African societies have introduced new complexities that complicate any straightforward application of African communitarian philosophy. Colonialism significantly reshaped African identity through the forced adoption of foreign languages, values, and institutions, and contemporary African societies continue to confront the consequences of these disruptions in identity formation (Kahaka & Maundeni, 2022; Amodu & Mohammed, 2022). In many urban and educated contexts, African individuals navigate spaces where traditional communal values and ancestral heritage are confronted by Western ideals of individualism, secularism, and modernity, producing increasingly hybridized conceptions of selfhood and identity (Amodu & Mohammed, 2022; Kahaka & Maundeni, 2022).

A counterargument could therefore be made that the blended model reflects a philosophical ideal rather than the lived reality of many contemporary Africans, and that grounding legal reform in it risks imposing a framework that does not reflect how Africans understand themselves today. This paper takes that counterargument seriously but offers two responses. First, as Kahaka and Maundeni (2022) demonstrate, individualism has always been present within African philosophical traditions, it is not an exclusively Western import introduced through colonialism. The blended model explicitly accommodates individual autonomy alongside communal embeddedness, and in that sense reflects rather than resists the direction of contemporary African identity (Kahaka & Maundeni, 2022, p. 58).

Second, the blended model is not deployed in this paper as a descriptive claim about how all Africans think today, it is deployed as a normative philosophical framework for grounding legal reform. Its value lies not in its universality but in its capacity to capture dimensions of personhood, namely, relational identity, communal belonging, dignity embedded in social con-

text, that existing legal frameworks fail to recognise and that remain deeply relevant to how images of African individuals and communities are understood, used, and misused in global digital markets (Kahaka & Maundeni, 2022; Amodu & Mohammed, 2022; Bayuo, 2025).

Ultimately, the blended model is not adopted in this paper merely as a philosophical preference, it is adopted because it is the only framework adequate to what this paper is arguing. This paper's central claim is that images are more than property and more than personal data; they are carriers of personal identity, relational belonging, historical memory, and communal significance simultaneously. A purely individualistic framework, whether grounded in Western property law, data protection, or privacy rights, can only ever see one dimension of an image; the individual's personal stake in their own likeness (Synodinou, 2014; Koryogdiev, 2025). Under both the GDPR's dataprotection model and the civillaw personalityrights model, image rights are structured around the individual's informational privacy, dignity, autonomy, and personal control over their likeness (Koryogdiev, 2025). Such frameworks do not recognize the family whose history the image carries, the community whose cultural identity it embodies, or the collective memory it represents (inferred from Koryogdiev, 2025; Synodinou, 2014).

The blended model, by recognizing individuals as simultaneously autonomous and relationally embedded, is the framework best suited to the specific argument this paper advances, and therefore the most appropriate foundation for a legal regime that responds to the full depth of harm caused when African images are extracted, decontextualized, and commercialized without consent or recognition (Kahaka & Maundeni, 2022; Menkiti, 1984; Amodu & Mohammed, 2022). This is a legal necessity rather than a philosophical indulgence.

III. KENYA'S LEGAL APPROACH TO IMAGE RIGHTS

Kenya does not possess a dedicated statutory framework that expressly protects an individual's image or likeness. Instead, protection arises from multiple overlapping instruments such as the Constitution of Kenya (2010), the DPA (2019), the Copyright Act (2001), and judicial interpretation, resulting in a fragmented and largely reactive framework, through which individuals must piece together constitutional principles, privacy rights, and limited statutory remedies to challenge the unauthorized use of their likeness.

This fragmentation within Kenya's legal framework is not accidental; it reflects deeper conceptual assumptions inherited from the Anglocommonlaw tradition, particularly its individualistic understanding of property (Honoré, 1961; Mamdani, 1996). In this tradition, property is defined not by the object itself but by a bundle of rights held by an individual: possession, use, control, transfer, exclusion, and commercial exploitation (Honoré, 1961; Waldron, 2010; Kariuki, 2016). This rights-based orientation privileges commodification and market-driven logic over relational understandings of identity and value, and because colonial legal systems treated property through this lens (Mamdani, 1996; Chanock, 1986), it shaped how post-colonial Kenya came to regulate creative works, images, and identity-related materials.

When applied to images, the bundle of rights model reveals that control over a visual representation is allocated according to proprietary entitlements rather than the personal or social meaning of the image. Kenya's current legal framework allocates these entitlements unevenly; the Copyright Act vests control primarily in the photographer or creator, while the DPA affords the depicted individual certain rights over their personal data. Yet neither framework, alone or together, provides adequate conceptual space for recognizing the subject's deeper interests in how their image is used, represented, and circulated, interests that go beyond data processing rules or creative ownership.

The result is a legal landscape in which an individual's image is simultaneously governed by competing frameworks; copyright law vesting control in the photographer, data protection law vesting consent rights in the depicted individual, and constitutional provisions on dignity and privacy recognising the individual's intrinsic worth and right to control their personal sphere. These frameworks do not operate in concert; they pull in different directions, allocate entitlements to different parties, and rest on different conceptual foundations, reflecting the bundle of rights model's allocation of control according to proprietary entitlements rather than the personal and social meaning embedded in the image. Courts have attempted to navigate this fragmentation through judicial interpretation, but the underlying conflict remains unresolved. The sections that follow examine each of these frameworks in turn; constitutional protections, statutory provisions, and judicial interpretation, mapping both what they offer and where they fall short. The reforms proposed in response to these gaps are developed in Part VI of this paper.

A. Constitutional Protection: Dignity, Privacy, and Property

At the heart of constitutional protection for image rights are three fundamental rights: the right to human dignity, the right to privacy, and the right to property (Constitution of Kenya, 2010, arts. 28, 31, 40). These provisions are intentionally broad, allowing them to be interpreted and applied to circumstances not anticipated at the time of enactment (Ambani, 2020), including the contemporary challenges posed by digital image circulation and global commercialization.

The right to human dignity establishes that every individual possesses intrinsic worth that the law must recognize and protect, reflecting the inherent value of the person beyond mere social or economic function (Constitution of Kenya, 2010, art. 28). This breadth has allowed courts to interpret dignity expansively, acknowledging that aspects of a person's identity, such as their image, name, and likeness, are intimately connected to

personality, selfhood, and social standing, and that misuse or unauthorized dissemination of these attributes can constitute a direct affront to personal dignity (T.O.S. v. Maseno University & 3 Others, 2016; Ann Njoki Kumena v. KTDA Agency Ltd, 2019). Complementing this, the right to privacy protects individuals against intrusion into their private sphere, encompassing unauthorized use or dissemination of personal information, including visual representations. Judicial decisions consistently highlight that consent is central to lawful publication or exploitation of images, reinforcing the principle that individuals retain control over how their personal attributes are accessed and employed (Jessica Clarise Wanjiru v. Davinci Aesthetics & Reconstruction Centre & 2 Others, 2017; T.O.S. v. Maseno University & 3 Others, 2016).

Moreover, Article 40 of the Constitution, which guarantees the right to property, can be relevant to image rights, particularly when a person's likeness is commercially exploited without consent. In practice, however, this provision is invoked relatively infrequently, usually only where the image is treated as a commodified asset and economic interests are directly implicated (Ann Njoki Kumena v. KTDA Agency Ltd, 2019). Its broad wording nevertheless creates latent potential for wider application. As jurisprudence develops and the commercial dimensions of image exploitation become more pronounced, Article 40 may increasingly provide a constitutional basis for recognizing the individual's economic interest in their own likeness alongside the protections already afforded by dignity and privacy.

Together, these constitutional protections establish a multidimensional framework for image rights, emphasizing both personal and, in certain contexts, economic dimensions, and situating the individual as the primary rights-holder over aspects of their identity. Their intentionally broad drafting is a strength rather than a limitation; it creates genuine judicial space for courts to develop a coherent image rights doctrine by reading Articles 28, 31, and 40 conjunctively, giving purposive effect to

constitutional guarantees in contexts their drafters could not have fully anticipated. The question that follows is not whether the Constitution provides adequate foundations for image rights protection, it does, but whether those foundations have been consistently and fully realized through statutory frameworks and judicial application. It is to those questions that the sections below turn.

B. Statutory Protection and its Limitations: The Data Protection Act and the Copyright Act

The DPA was enacted to give effect to Article 31(c) and (d) of the Constitution, which guarantees every person the right to privacy. The Act provides a comprehensive framework regulating the collection, storage, processing, and disclosure of personal data, ensuring that these activities are lawful, fair, and secure (Data Protection Act, 2019, Part III and IV). In doing so, it operationalizes the constitutional right to informational privacy, translating abstract guarantees into enforceable obligations. What is particularly significant for image rights is that the DPA explicitly recognizes photographs and other visual representations as forms of personal data (Data Protection Act, 2019, s. 2), situating the individual as the primary rights-holder, and placing accountability on anyone who collects or uses images of identifiable persons.

Under the DPA, personal data is defined broadly as any information relating to an identified or identifiable natural person, encompassing both direct and indirect identifiers, including images and other visual representations capable of revealing a person's identity (Data Protection Act, 2019, s. 2). Photographs and video recordings featuring identifiable individuals therefore qualify as personal data, and their collection, publication, or dissemination is subject to the Act's requirements, including obtaining informed consent and ensuring lawful and fair processing; notwithstanding whether it is for personal, institutional, or commercial purposes (Data Protection Act, 2019, ss. 25, 32). This

statutory recognition is vital because it aligns legal protection with contemporary realities; digital images can be copied, distributed, and monetized with unprecedented speed and scale, heightening the risk of unauthorized use.

While the DPA centers on the depicted individual, the Copyright Act, 2001, approaches images from a fundamentally different perspective by prioritizing the rights of the creator rather than the subject. Under section 2 of the Act, a photograph is expressly classified as an artistic work. By virtue of section 22, such artistic works are eligible for copyright protection, granting exclusive rights to reproduce, distribute, and otherwise exploit the work to the author; that is, the person responsible for composing the image which could be the photographer or creator (Copyright Act, 2001, ss. 2, 22). Section 32 further recognizes the moral rights of authors, which exist independently of economic rights and persist even after the rights are transferred, and include the right to claim authorship and to object to any distortion, mutilation, or modification of the work prejudicial to the author's honor or reputation.

Critically, these rights attach solely to the creator of the image, not the individual depicted, producing a structural tension between the individual as data subject under the DPA and the creator as rights-holder under copyright law (Copyright Act, 2001, s. 32).

In the Kenyan context, this tension is magnified by the lack of a clear statutory mechanism that harmonizes these overlapping interests, leaving individuals with limited practical recourse when their image is used for commercial gain. To illustrate the tension between individual control and the rights of creators, consider the case of my father's images. A number of his images, which capture Kenyan sports history and document his personal journey as a cricketer, are currently licensed through U.S.-based platforms namely Getty Images and Alamy. Although these platforms operate outside Kenya's jurisdiction, they exemplify a fundamental tension both locally and globally. Under data protec-

tion law, the individuals depicted are the owners of their personal data, granting them control over how the images are collected, used, and disseminated. Yet under copyright law, the photographer is the owner of the images, holding the exclusive right to reproduce, distribute, and commercially exploit the works. In practice, this means that an individual whose image captures a defining moment in their personal and national history can find themselves entirely without legal recourse, not because the law ignores them, but because the law speaks to them through two conflicting frameworks that pull in opposite directions, leaving the question of who truly controls the image without a coherent answer.

While courts have, on occasion, leaned toward protecting the individual's privacy and dignity interests over the photographer's commercial and intellectual property rights, a pattern examined in greater detail in Part III, section C of this paper, the underlying legal conflict remains unresolved. There is currently no statutory mechanism to determine which framework prevails when the two conflict, and the absence of such a mechanism leaves the outcome dependent on judicial discretion rather than clear legal principle. The result is a landscape in which individuals are formally protected in theory but practically vulnerable in fact. The deeper problem, however, is not merely the conflict between these two frameworks, it is what both share. Whether an image is treated as personal data under the DPA or as creative property under the Copyright Act, it is reduced to a single dimension, a data point or an asset, neither of which captures what an image represents in African contexts. An individual's image carries their relational identity, their historical significance, and their embeddedness within family and community. These dimensions of meaning are invisible to both frameworks as currently conceived, as they are rooted in Western legal traditions that conceive of images through individualistic categories of property and data, frameworks that were never designed to recognize the relational, historical, and personal dimensions of

meaning that images carry in African contexts.

The solution this paper proposes is an interpretive framework grounded in African conceptions of personhood that provides courts and legislators with a richer lens through which to read and apply both statutes, and on the basis of which targeted amendments can be made to give that richer understanding legal force.

C. Judicial Interpretation of Image Rights in Kenya

In the absence of a dedicated statutory regime, Kenyan courts have drawn on precisely the constitutional provisions discussed above; dignity, privacy, and property, to interpret and enforce image rights, filling the gaps left by the fragmented legislative landscape. The emerging jurisprudence is instructive, and this paper builds on it rather than departing from it.

In T.O.S. v. Maseno University & 3 Others (2016), the court underscored that publishing or using an individual's images without consent infringes the constitutional right to privacy, emphasizing that the individual alone determines when, how, and under what conditions their private life may be accessed. Building on this foundation, in Ann Njoki Kumena v KTDA Agency Ltd (2019), the court affirmed that a person has the right to control the use of their image, name, or likeness, and that consent is required before such attributes are deployed for commercial or publicity purposes. In Jessica Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre & 2 Others (2017), the court identified three components necessary to establish a claim for the unauthorized use of name or image, the use of a protected attribute, its deployment for an exploitative purpose, and the absence of consent. Through this approach the court further distinguished the difference between the right to privacy, available to all individuals to guard against non-consensual use, and the right of publicity, which confers exclusive commercial control over one's image. More recently, in Wanjiru v Machakos Univer-

sity (2022), the court reiterated that a person's image constitutes one of the principal attributes of their personality and that individuals retain the right to protect and control its use.

Taken together, these decisions reveal a consistent judicial pattern, where the individual's privacy and dignity interests have come into conflict with the photographer's commercial and intellectual property rights, courts have repeatedly prioritized the former. This is significant not only as a matter of privacy law but as an implicit judicial recognition that the subject's constitutional interests in their image take precedence over the creator's statutory rights under the Copyright Act, 2001. This paper builds on that recognition rather than departing from it, and the framework proposed in subsequent sections seeks to give it more consistent, coherent, and far-reaching legal expression.

Yet this consistent prioritisation of privacy rights, while commendable, remains insufficient to address the full depth of the problem. Judicial protection of privacy is fundamentally defensive and reactive. It responds to a specific intrusion after it has occurred, orders its cessation, and awards compensation for the discrete violation. What it cannot do is address the structural and ongoing nature of the harm that occurs when an individual's image, carrying their relational identity, their historical significance, and their embeddedness within family and community, is extracted from its context, stripped of its meaning, and circulated as a commodity (even on global platforms far beyond the reach of any single court order). A judgment in favor of the individual in one case does not restore narrative authority over how their image circulates more broadly, does not ensure their image is treated with the dignity it carries, and does not prevent the same harm from recurring in a different transaction on a different platform.

D. Towards an African-Centered Approach to Image Rights

The interplay between constitutional guarantees, statutory

provisions, and judicial interpretation reveals both the promise and the limitations of Kenya's current legal landscape. Despite meaningful protections within privacy law and growing judicial recognition of personality interests, the framework remains fragmented, often forcing image-related disputes into narrow categories of property, data, or commercial exploitation.

Building on the conceptual framework discussed earlier (Kahaka & Maundeni, 2022), a personhood-centered approach provides a coherent pathway for understanding image rights in Kenya. Rather than treating images solely as objects of ownership or as data points, this perspective recognizes them as extensions of individual identity, autonomy, and social narrative, situating image rights within a relational understanding of personhood, which acknowledges both the embeddedness of individuals within communities and their capacity for independent agency.

Developing a personhood-centered approach would require harmonizing constitutional values with the operational logics of data protection and copyright law, allowing the law to balance individual autonomy with legitimate creative and commercial interests, while remaining consistent with African relational conceptions of personhood. Later sections of this paper build on this orientation, proposing ways in which the law may be interpreted or reformed to give effect to this framework. Consequently, in practice, a legal structure grounded in personhood would empower individuals with substantive control over their images, provide clearer obligations and safeguards for creators and institutions, and offer a robust response to the challenges posed by digital, cross-border, and increasingly commercialized image circulation. To assess how such a framework might be shaped, strengthened, or distinguished from existing global models, it becomes necessary to examine how other jurisdictions conceptualize and regulate image use.

IV. COMPARATIVE ANALYSIS OF IMAGE RIGHTS

Understanding how different legal systems regulate image use is essential for situating Kenya's emerging discourse within a broader global context. This section examines three jurisdictions: the European Union (EU), France, and South Africa, selected based on their specific legal connections to Kenya and the distinct but complementary perspectives each offers on image protection.

The EU serves as the primary international reference point given that Kenya's Data Protection Act, 2019, borrowed substantially from the GDPR in its structure, definitions, and consent framework, making it the natural starting point for examining the architecture Kenya's own law is built on (Data Protection Act, 2019; General Data Protection Regulation, 2016/679). France, meanwhile, offers the most developed personality rights tradition in the civil law world, a subject-centered model of image protection grounded in dignity and autonomy rather than data processing rules, providing a direct reference point for the subject-centered framework this paper proposes for Kenya (Synodinou, 2014). South Africa, as an African common law jurisdiction whose transformative Constitution shares a closely analogous architecture with Kenya's, centering dignity and privacy as foundational rights, offers the most contextually proximate model for examining how dignity-based image protection currently operates within an African legal system (Constitution of the Republic of South Africa, 1996; Constitution of Kenya, 2010).

Although no single jurisdiction offers a complete model for African societies, each contributes valuable doctrinal insight that informs the proposals advanced in Part VI of this paper; whether by testing the reach of a data-based model, demonstrating a subject-centered alternative, or exposing the limits of dignity-based protection left to case-by-case enforcement. Crucially, the comparative analysis is not conducted to identify a framework for wholesale adoption; it is conducted to identify what is

useful, what must be adapted, and where African conceptions of personhood and dignity require Kenya to depart from all three models entirely.

A. Image Rights in the European Union

Kenya's Data Protection Act, 2019 borrows substantially from the GDPR in its structure, definitions, and consent framework, making the EU not only the most direct international reference point for Kenya's existing data protection architecture but also a diagnostic comparator (Data Protection Act, 2019; General Data Protection Regulation, 2016/679).

Examining the GDPR in depth therefore serves to illuminate the foundations of Kenya's current approach, including its embedded limitations, since any limitation in the GDPR's underlying conception of the person is a limitation Kenya's law is likely to have inherited. It also helps to test whether even the most developed individual-rights-based data protection framework in the world can accommodate the relational, historical, and communal significance embedded in an individual's image, or whether this is a limitation built into the paradigm itself, one that cannot be resolved simply by refining Kenya's existing consent and processing provisions.

At the core of EU law, the GDPR establishes the protection of personal data, including images, as a fundamental right, derived from Article 8 of the Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights of the European Union, 2000, art. 8). Article 4(1) of the GDPR explicitly defines personal data as 'any information relating to an identified or identifiable natural person', which includes images where individuals can be recognized (General Data Protection Regulation, 2016/679, art. 4(1)), and for the collection and processing of such personal data, the consent of the data subject is central (General Data Protection Regulation, 2016/679, art. 6(1)(a)). Consent is defined as 'any freely given, specific, informed, and unambiguous

indication of the data subject's wishes', under Article 4(11), while Article 7 sets out the conditions for obtaining and demonstrating valid consent (General Data Protection Regulation, 2016/679, arts. 4(11), 7). The European Data Protection Board has further clarified that these criteria apply specifically to the processing of personal data including photographs, ensuring that any commercial or public use of images involving identifiable individuals must meet high standards of transparency and voluntariness (European Data Protection Board, 2020).

Despite its focus being primarily on privacy, the protection of personal data, encompassing identifiable images as part of an individual's personal information, the EU does not recognize a single, unified personality or image right. Instead, protection is derived from a combination of national laws, human rights obligations, and data protection regulations, with the GDPR serving as the most influential supranational instrument in this regard (Synodinou, 2014; Voigt & von dem Bussche, 2017).

National courts across EU Member States interpret and enforce these provisions in conjunction with domestic laws on personality and privacy rights. Civil-law countries, such as Germany, Italy, and France, often situate image protection within a hybrid system, recognizing both the dignitary and economic aspects of an individual's image, sometimes drawing analogies with copyright law to protect the economic value of images (Synodinou, 2014, p. 184). By contrast, the United Kingdom, which is no longer bound by the GDPR following its withdrawal from the EU, offers only piecemeal protection through the torts of breach of confidence or passing off (Synodinou, 2014, pp. 186-187). That even a jurisdiction operating outside the EU's data protection regime, and drawing on a distinct common-law tradition, arrives at a similarly fragmented and individual-focused model of image protection suggests that the limitation is not confined to the GDPR's specific architecture, but reflects a broader difficulty within Western legal traditions in accounting for the fuller meaning an image can carry.

While the EU offers a robust, multi-layered framework for regulating images, its orientation toward personal data protection and human dignity confirms the limitation this comparison set out to test. By framing image rights primarily as a subset of privacy or data protection, the EU model is structurally unable to capture the relational, historical, and personal significance embedded in an individual's image, not because its provisions are poorly designed or under-enforced, but because informational self-determination and consent, however rigorously applied, are simply not the conceptual tools that task requires. This is the central lesson the comparison yields, because Kenya's DPA was modelled on the GDPR, it inherits the same conceptual ceiling, and the DPA cannot capture the full depth of harm to the individual, specifically, the harm to their relational identity, historical significance, and personal embeddedness. Strengthening consent standards or harmonizing enforcement, as the EU has continued to do, cannot close this gap, because the gap is paradigmatic rather than procedural: no degree of refinement to a privacy-based model can supply what a privacy-based model is not designed to protect.

Consequently, the EU comparison demonstrates that image-rights protection cannot be achieved simply by adopting or refining a data protection model, however sophisticated. For African countries like Kenya, this underscores the need to critically evaluate, adapt, or depart from EU models, rather than adopting them wholesale, recognizing instead that an individual's image carries meaning that extends beyond personal data, it reflects who they are within their family, community, and historical moment, and the law must recognize that fuller meaning when assessing harm.

B. Image Rights in France

Where the EU addresses images primarily as personal data, France's legal tradition approaches them as expressions of personhood, making French law a critical complement to the GDPR

analysis and a direct reference point for the subject-centered image rights framework this paper proposes for Kenya.

In France, the right to one's own image is firmly anchored in the broader framework of personality rights, reflecting the civil law tradition that prioritizes individual dignity. Article 9 of the French Civil Code establishes that 'everyone has the right to respect for his private life' (Code civil [French Civil Code], art. 9), a provision that has been judicially interpreted to encompass protection over a person's image (Synodinou, 2014). Together, these provisions make clear that a person's image is considered an inalienable attribute of their personality, inseparable from their dignity and autonomy, and therefore cannot be reproduced, disseminated, or commercially exploited without proper consent (Ann Fitzgerald, 2019), a principle that resonates directly with the subject-centered approach this paper advocates for Kenya.

The exclusivity of this right is emphasized by jurisprudence, which requires that prior permission must be sought for any use of an individual's image, whether in public or private settings, and regardless of the number of individuals depicted or the context in which they appear (CIPIT, n.d.). French courts have extended this protection beyond obvious physical identifiers, recognizing that a person can be identifiable by tattoos, distinctive features, or contextual elements such as settings and décor (Ann Fitzgerald, 2019). The courts have also stressed that consent must be express, specific, and in writing, and should detail the scope of permitted use, the territorial coverage, the intended purpose, and the duration for which consent is granted, typically limited to a reasonable term of 2 to 3 years (Ann Fitzgerald, 2019). While the law allows consent to be granted free of charge or in exchange for compensation, it cannot be assigned indefinitely (Ann Fitzgerald, 2019), underscoring the inalienable nature of the right.

French law also distinguishes between the dignitary and patrimonial dimensions of image rights, mirroring the duality discussed in broader European civil law systems. The non-patri-

monial, or 'dignity', aspect focuses on the protection of personal autonomy and the right to control one's own representation, ensuring that unauthorized reproduction or dissemination does not cause personal harm (Synodinou, 2014, pp. 183-184). The patrimonial, or economic, aspect concerns the commercial exploitation of the image. Courts have sometimes adopted contractual or tort-based solutions to govern these economic rights, particularly when disputes arise regarding unauthorized commercial use (Synodinou, 2014, pp. 183-184). However, the French law does not recognize commercial image rights as autonomous property, unlike US-style publicity rights which constitute a freestanding intellectual property right that can be owned, licensed, and transferred independently of the person. Instead, the economic interest in one's image derives its legal force from the personality right itself, remaining attached to the person and incapable of full separation from their identity. Commercial exploitation of an image is therefore governed not by property logic but by personality logic, that is, the subject retains an inalienable connection to their image even where commercial use has been authorized (Synodinou, 2014, pp. 183-184).

The practical application of these principles has been shaped by case law emphasizing both the context of image capture and the identifiable nature of the person depicted. Infringement is considered to occur when the image can reasonably identify an individual, even if the reproduction is partial or incidental, or if the image is captured in public spaces (Ann Fitzgerald, 2019). For public figures, the law balances the protection of personal dignity with freedom of expression, allowing certain press coverage or documentary use while maintaining stringent limits on commercial exploitation without consent. This nuanced approach ensures that the rights of individuals are respected without unnecessarily restricting legitimate reporting or artistic expression (Ann Fitzgerald, 2019).

Despite its coherence and the strong protection it affords, the French model ultimately reflects the values and social imag-

inaries of a European civil-law tradition, particularly its individualistic conception of personhood, dignity, and autonomy. This framework works remarkably well within its own cultural and jurisprudential context. However, its underlying assumptions do not translate seamlessly into African societies, where identity, representation, and the meaning of an 'image' often extend beyond narrow individualistic categories to encompass the individual's lineage, relational embeddedness, and historical significance. As a result, simply borrowing or transplanting the French approach would repeat a long-standing pattern in African legislative practice; the uncritical adoption of Western legal norms without assessing their cultural fitness or normative foundations. The strength of the French *droit à l'image* should not obscure the need for African jurisdictions to craft models responsive to local notions of dignity understood through relational personhood, historical significance, and personal embeddedness, and the socio-economic realities shaping image use on the continent. In this sense, the French framework provides valuable doctrinal insight, but it cannot serve as a complete blueprint for an African-centered regulation of image rights.

C. Image Rights in South Africa

As an African common law jurisdiction whose transformative Constitution centers dignity and privacy in terms closely analogous to Kenya's own constitutional framework, South Africa offers the most contextually proximate comparator in this analysis (Constitution of the Republic of South Africa, 1996, ss. 10, 14; Constitution of Kenya, 2010, arts. 28, 31). South Africa's legal framework does not establish image rights as an independent category of protection; rather, the regulation of image-based harm is embedded within constitutional rights, particularly dignity (Constitution of the Republic of South Africa, 1996, s. 10) and privacy (s. 14), and the Roman Dutch common-law tradition of personality rights. The principal mechanism for enforcing these rights is the actio injuriarum, a civil remedy designed to

address intentional and wrongful infringements of personality interests such as dignity, reputation, and privacy (Neethling, 2005; Burchell, 2009), and consistently applied by the courts in cases involving image-based harm (O'Keeffe v Argus Printing and Publishing Co., 1954; Wells v Atoll Media (Pty) Ltd, 2009). Examining this framework reveals both the practical potential of dignity-based image protection within an African constitutional system and its limits. This approach remains anchored in a western-individualized conception of personhood, and its protection is realized only reactively through case-by-case judicial remedy after harm has already occurred, rather than through proactive recognition within the law itself; limits that Kenya's African-centered framework must directly address.

South African courts have long accepted that the unauthorized publication of a person's image may amount to an infringement of dignity or privacy. In O'Keeffe v Argus Printing and Publishing Co. Ltd (1954), the court held that the use of the plaintiff's photograph and name in a commercial advertisement without her consent constituted an injuria. The judgment underscored that such use could amount to 'arrogant, ignominious and offensive treatment', depending on factors such as the context of publication and the personal attributes of the plaintiff. This early decision confirmed that the appropriation of a person's likeness for commercial advantage can infringe dignity even without a proprietary image right.

The principle was later reaffirmed in Angella Wells v Atoll Media (Pty) Ltd & Another (2006), where the Western Cape High Court held that the commercial exploitation of a person's image without consent may constitute an unjustifiable violation of both dignity and privacy. The court emphasized that when a photograph is used to market a publication or otherwise generate profit, the individual's personality interests require heightened protection and respect.

This jurisprudence operates within a broader privacy framework, which recognizes four categories of invasion: intrusion,

publication of private facts, false light, and appropriation (Prosser, 1960; Case Western Reserve University Law Library, n.d.). Appropriation, which is defined as the use of another person's name, image, likeness, or other identifying attributes for the benefit of the user, is the most relevant category for image-based harms (Prosser, 1960; Case Western Reserve University Law Library, n.d.). In such cases, the actio injuriarum provides a flexible set of remedies, including damages and interdicts, enabling courts to respond to a variety of unauthorized uses of personal images (Neethling, 2005; Burchell, 2009).

While South Africa's jurisprudence demonstrates the effectiveness of dignity-based protection, as discussed, it remains anchored in a legal tradition inherited from Roman Dutch and European frameworks. The actio injuriarum and the constitutional interpretation of dignity center an individualized, rights-bearing notion of the self, rather than an African-rooted understanding of personhood as relational, communal, and historically situated. As a result, although the courts provide robust remedies for unauthorized image use, particularly in cases of commercial exploitation, the law does not fully engage with the ways images in African contexts may carry relational identity, evoke historical significance, or reflect the individual's personal embeddedness within their community. The model is therefore instructive but incomplete for jurisdictions seeking a culturally grounded, African-centered approach to representation and image-based harms.

As briefly noted earlier, this reactive posture mirrors a challenge already identified within Kenya's legal landscape, where existing protections likewise depend on individuals initiating remedial action after harm has taken place. That South Africa's jurisprudence, arguably the most developed on the continent and grounded in a constitutional order closely analogous to Kenya's, has not moved beyond this reactive posture suggests the limitation is not particular to Kenya's institutional immaturity, but a broader feature of remedy-based, case-by-case approaches to im-

age protection. This reinforces the case for a framework that recognizes the fuller meaning of an individual's image proactively within the law itself, rather than relying on courts to reconstruct that recognition after the fact.

D. Key Insights from the Comparative Jurisdictions

Taken together, these jurisdictions offer three distinct but complementary approaches to regulating image use, each illuminating a different dimension of the problem Kenya faces. The EU model conceptualizes images through the lens of personal data, building a regime centered on individual control, consent, transparency, and accountability (General Data Protection Regulation, 2016/679). France develops a personality-rights doctrine that treats one's image as an inalienable extension of the self, grounded in dignity and autonomy, offering a subject-centered model that goes beyond data processing rules, grounding consent in personality rather than processing obligations (unlike the GDPR), to recognize the deeper personal interests at stake in image disputes (Synodinou, 2014). South Africa illustrates how dignity and privacy can function as anchors for image protection in a common-law African jurisdiction, within a constitutional framework closely analogous to Kenya's, though, as the analysis in Part IV, Section C of this paper shows, this protection is realized only reactively, through case-by-case judicial remedy, rather than through any proactive recognition within the law itself (Constitution of the Republic of South Africa, 1996; Constitution of Kenya, 2010).

Yet none of these frameworks fully capture the relational, historical, and personal significance embedded in an individual's image. They prioritize individual agency and personal autonomy, addressing what an individual's image represents chiefly as data, personality, or dignity in the abstract, without recognizing who that individual is within their family, community, and historical moment. Where they offer remedy at all, it is typically activated only after harm has occurred, leaving recognition

of image-based interests to litigation rather than embedding it within the law itself. They do not address the legacies of representational harm, extractive visual practices, and enduring power imbalances that continue to shape how African images circulate globally (Couldry & Mejias, 2019; Birhane, 2023). And while they demonstrate that dignity-based, non-proprietary approaches to image protection are possible, they reveal the absence of a framework that integrates African communitarian philosophies, historical consciousness, and contemporary digital realities.

The comparative analysis has therefore delivered precisely what it set out to, not a model for wholesale adoption, but a map of doctrinal possibilities and their limits. It shows Kenya what tools are available, where they fall short, and where African conceptions of personhood and dignity require a fundamentally different approach. This opens space for Kenya to articulate a more contextually grounded and normatively coherent model for image rights, one that draws from constitutional values while recognizing the lived social meaning of images within African communities. To understand why such a framework is urgently needed, it is necessary to confront the structural forces that shape how African images are produced, circulated, and appropriated in global digital systems, forces increasingly described through the lens of data colonialism.

V. DATA COLONIALISM AND AFRICAN IMAGES

Understanding how images of African individuals, whether public figures, cultural icons, or ordinary citizens, circulate across global digital infrastructures requires grappling with the deeper structural logics shaping contemporary data practices. Over the past decade, scholars such as Couldry and Mejias (2019) have conceptualized data colonialism as 'a new social order that mirrors historical patterns of extraction' (p. 1). In their view, contemporary digital systems do not merely gather information, they extract human experience itself, converting everyday social

life into commercial assets controlled by powerful institutions (Couldry & Mejias, 2019). This mode of extraction is uneven, replicating global hierarchies in which the Global South becomes a reservoir of cultural meaning, visibility, and value harvested for use elsewhere (Birhane, 2023; Milan & Treré, 2019).

In the context of image circulation, this theoretical lens illuminates how photographs of African people, including public figures, cultural figures, and ordinary citizens, are detached from their original contexts and integrated into global commercial ecosystems through well-established platform infrastructures. As this section demonstrates, images travel from the moment of capture through photographer agreements, wire agency partnerships, and contributor upload systems onto major stock photography platforms, where they are classified, priced, and licensed under terms that afford the depicted subject no role, right, or remedy in the transaction. Rather than being treated as heritage, memory, or repositories of lived identity and personal significance, these images are absorbed as marketable content that generates revenue for digital intermediaries, image agencies, and platform owners, often leaving those depicted with no control over how their identities are displayed, interpreted, or monetized (Birhane, 2023).

To unpack the consequences of this phenomenon, this section examines four interrelated dynamics: first, how global platforms extract and commercialize African images and the infrastructure through which this occurs; second, how this process erodes African narrative control, dignity, and identity; third, how Kenya's experience situates these dynamics within the broader global landscape and what pathways exist for reclaiming control; and fourth, the implications of these dynamics for Kenya's image rights debate. The commercial circulation of images of Steve Tikolo serves as a concrete illustration of these dynamics.

A. Extracting and Commercializing African Images

The extraction of African images for global consumption is neither accidental nor innocent; it reflects the foundational logic of data colonialism, in which human subjects, their social moments, and historical representations are converted into raw material for global digital markets (Couldry & Mejias, 2019). African images are disproportionately affected. Unlike many other regions, most African jurisdictions lack coherent legal frameworks for image rights, and Africa's historical positioning as a source of cultural content for global markets makes its visual heritage particularly vulnerable to extraction (Couldry & Mejias, 2019; Birhane, 2023). Once photographs capturing pivotal historical, social, cultural, or political moments across African countries enter repositories held by international stock agencies, photojournalistic archives, and digital licensing platforms, they often become available for worldwide licensing irrespective of their significance. Once incorporated into large repositories, these images are detached from the individuals depicted and the contexts from which they emerged (Birhane, 2023), and the individuals photographed, be it athletes, elders, cultural leaders, artists, or ordinary citizens, rarely have a voice in long-term circulation or in the profits derived from licensing (Birhane, 2023).

Understanding how this detachment occurs requires examining the commercial and contractual infrastructure through which images travel from the moment of capture to global circulation. Two of the world's leading stock photography platforms, Getty Images and Alamy, illustrate this infrastructure with clarity. While they differ in how they source content, they converge on the same legal outcome; the systematic exclusion of the image subject from the transaction entirely.

Getty Images sources content through multiple channels, most significantly through long-term partnerships with international wire agencies. Its agreement with Agence France-Presse (AFP), for instance, draws on a network of over 450 photog-

raphers across more than 150 countries, contributing content through over 70 partner agencies (Getty Images & AFP, 2026). Independent contributors may also upload content directly through Getty's online portal. In either case, once content is accepted, the contributor enters into an agreement that transfers to Getty the exclusive worldwide right to license the images and determine pricing unilaterally, in return for a royalty of between 15% and 45% of each sale (Getty Images Contributor Agreement v5.1, n.d.). Alamy, by contrast, operates almost exclusively through independent contributor uploads, with no comparable wire agency infrastructure (Alamy Contributor Terms and Conditions, 2023). Nevertheless, its contractual terms mirror Getty's in their essential effect, contributors grant Alamy full authority to negotiate all terms of licenses and reproduction rights, including the fee, duration, and scope of any license, at its absolute discretion (Alamy Contributor Terms and Conditions, 2023).

In both cases, the person depicted in the image is entirely absent from this transaction. This absence is structurally encoded in how both platforms classify and license content. Images depicting real people at news, sports, or cultural events are categorized as editorial content, and under this classification, neither Getty nor Alamy requires model or property releases from the subjects depicted (Getty Images, 2024b; Alamy, 2024). The subject has therefore given no consent to the licensing, has no contractual standing to object to or withhold permission for a specific use, and has no entitlement to share in the proceeds (Getty Images Contributor Agreement v5.1, n.d.; Getty Images, 2024b; Alamy Contributor Terms and Conditions, 2023). The contract exists exclusively between the photographer, the platform, and the buyer. As a result, a photograph of a Kenyan athlete or cultural figure can be uploaded by a photographer, accepted by a platform, priced at hundreds of dollars per license (Getty Images, 2024c), and sold to buyers across the world, with value flowing entirely among the photographer, the platform, and the purchaser.

Commercial mechanisms further compound this exclusion by stripping images of their context. African images are reduced to generic commodity categories through metadata labels such as 'African athlete' or 'Kenyan man or woman', which prioritize marketability over the lived realities these images represent (Milan & Treré, 2019; Birhane, 2023). This abstraction exemplifies the 'appropriation of life through data' described by Couldry and Mejias (2019), in which richness, context, and agency are subordinated to extractive value (p. 1). A clear illustration of this dynamic is evident in the commercial availability of photographs of Steve Tikolo on Getty Images and Alamy. These images capture defining moments both in his personal life and in Kenya's cricket history, yet they are presented as purchasable commodities with no mechanism for him to control their usage or receive financial benefit, described primarily through market-oriented metadata that erases the significance embedded in these moments. Across the continent, this logic repeats, value flows outward to platforms and agencies, while African subjects remain excluded from the economic ecosystems built around their own likenesses (Ijuo, 2025).

Viewed through the lens of African personhood, the harm extends beyond economic spheres. When an image is extracted from its social context and circulated as a commodity, what is lost is not merely a revenue stream, it is a person's authority over how they are seen, remembered, and represented within their community and beyond (Amodu & Mohammed, 2022; Kahaka & Maundeni, 2022). The platform infrastructure described above does not merely fail to protect this interest; it is structurally designed to ignore it, treating the image as an asset belonging to whoever holds the copyright while rendering the subject entirely invisible to the transaction, an individual whose image carries not merely personal data but their relational identity, historical significance, and personal embeddedness within family, community, and cultural memory (Birhane, 2023; Ijuo, 2025).

B. Impact on the Narrative Control, Dignity and Identity of African Image Subjects

The platform infrastructure documented above has consequences for how individuals understand and assert their own identity, dignity, and narrative authority. When an individual's image is extracted from its context and circulated as a commodity, what is lost is not merely a revenue stream or a data point, it is a set of markers through which that individual understands and expresses who they are. In African contexts, these markers are concrete and philosophically grounded. Lineage and blood ties that connect an individual to a multigenerational continuum, names that carry ancestral significance and communal standing without which a person loses their capacity for continuity across generations (Menkiti, 1984, pp. 174-175), geographic and community rootedness through which personhood is constituted (Menkiti, 1984, p. 171), and tribal or ethnic belonging that situates the self within a relational web of meaning (Menkiti, 1984, p. 171; Kahaka & Maundeni, 2022, p. 61). When an image is reduced to a metadata label (such as 'African athlete' or 'Kenyan man') these markers are not merely overlooked; they are actively erased, replaced by a generic commercial category that bears no relation to the individual's actual identity or significance (Milan & Treré, 2019; Birhane, 2023).

This dynamic is vividly illustrated by the circulation of Steve Tikolo's images on Getty Images and Alamy. His photographs capture transformative moments, victories that inspired national pride, leadership moments that shaped Kenyan sporting culture, personal milestones significant to our family and community. Yet on these platforms, they are presented as purchasable commodities described primarily through market-oriented metadata, stripped of the narrative richness that makes them significant. What is erased is not just context, it is his lineage as one of Kenya's most celebrated cricketers, the historical significance of the moments captured, and his embeddedness within a sporting and national community whose story these images carry. This

pattern, as Birhane (2023) demonstrates, repeats across the continent, with individuals becoming passive nodes within systems that extract value while marginalizing the original agents.

The broader consequence is what scholars of data colonialism have described as symbolic dispossession; a process by which individuals encounter their own visual heritage through the priorities of foreign actors rather than through self-determined frameworks (Milan & Treré, 2019; Couldry & Mejias, 2019). Narrative control becomes a contested space where visibility does not guarantee agency, as African individuals remain perpetually present in global image markets yet entirely absent from the decisions that shape how their stories are told, interpreted, and circulated. They are seen everywhere but heard nowhere (Birhane, 2023; Couldry & Mejias, 2019). This absence has consequences that extend beyond the individual transaction. By controlling the circulation and interpretation of African images, global platforms shape how African histories are experienced and understood globally, extending the colonization of human life through data systems into the very realm of memory and identity formation (Couldry & Mejias, 2019).

Yet existing legal frameworks are not equipped to recognize or remedy this depth of harm. Privacy law responds to intrusion; copyright law responds to unauthorized reproduction; data protection law responds to unlawful processing. None of these categories reaches the harm that occurs when an individual's image is stripped of that meaning and reduced to a marketable commodity, despite carrying their lineage, their name's ancestral significance, their geographic and cultural rootedness. The law, as currently conceived, can see the transaction but cannot see what is lost in it. It is precisely this gap between the harm that image extraction causes to the individual and the harm that existing law is capable of recognizing, not by abandoning existing frameworks but by reinterpreting and extending them through a richer understanding of what an individual's image actually is and means.

C. Kenya in the Global Landscape and Pathways for Reclaiming Control

Kenya's experience exemplifies broader patterns of data colonialism across the Global South, where digital infrastructures enable the extraction and global circulation of data while interpretive and commercial authority resides primarily with entities headquartered in the Global North (Milan & Treré, 2019; Birhane, 2023). Kenyan images are disproportionately represented on global platforms, yet the individuals depicted remain largely excluded from decisions regarding circulation, licensing, and contextual interpretation of their own likenesses (Milan & Treré, 2019; Birhane, 2023). This dynamic mirrors historical extraction practices, albeit through digital means, and underscores the persistence of structural asymmetries in global information flows (Kwet, 2019).

While the DPA establishes privacy and consent obligations and situates the individual as the primary rights-holder (Data Protection Act, 2019, ss. 2, 25, 32), this paper argues that it cannot capture the fuller dimension of harm that image extraction causes, specifically, the harm to an individual whose image carries their relational identity, historical significance, and personal embeddedness, dimensions that the DPA's individual-centered data processing framework was not designed to recognize. This conceptual gap is further compounded by the Copyright Act, 2001, which centers the photographer as the exclusive rights-holder (Copyright Act, 2001, s. 32) rather than the subject depicted, leaving the individual with limited recourse when their image is commercially exploited. While Kenyan courts have consistently prioritized the individual's privacy and dignity interests over the photographer's commercial rights, this pattern remains insufficient to address the structural and ongoing nature of the harm identified above. Both frameworks also operate primarily within national borders, leaving Kenyan individuals without effective recourse against platforms operating from foreign jurisdictions.

In addition, standardized metadata systems and licensing categories further flatten complex contexts, prioritizing global discoverability and market utility over the relational identity and personal significance of the individuals depicted (Birhane, 2023; Knowledge Commons Brazil, n.d.). The consequence is a profound dislocation where African subjects are rendered passive objects in markets built on their own images (Birhane, 2023), while the relational and individual dimensions of their identities remain unprotected.

Addressing these challenges does not require constructing an entirely new legal regime. Rather, it requires the reinterpretation and integration of existing frameworks, constitutional, statutory, and regional, through an African philosophical lens that recognizes individuals as both autonomous and relationally embedded.

At the national level, this means reading Kenya's constitutional provisions on dignity, privacy, and property conjunctively rather than in isolation, and extending the DPA consent and processing obligations to more fully account for the depth of harm that image extraction causes to the individual; specifically, harm to their relational identity, historical significance, and personal embeddedness, and reinterpreting the Copyright Act's existing moral rights framework to recognize the subject's narrative and identity interests alongside the photographer's creative rights, with the specific proposals and their compatibility with international IP obligations developed in Part VI of this paper (*Constitution of Kenya*, 2010, arts. 28, 31, 40; *Data Protection Act*, 2019; *Copyright Act*, 2001, s. 32). Digital dignity must be central to this reinterpretation, granting individuals meaningful agency over the capture, dissemination, and monetization of their images.

Consent frameworks must similarly be reimagined as a further dimension of this national reinterpretation. The DPA already establishes that consent must be free, specific, informed, and unambiguous (*Data Protection Act*, 2019, ss. 25, 32), a solid foundation, but one that is insufficient in the specific context of

image rights for two reasons. First, the DPA's consent requirement does not account for the context in which an image was originally created. It asks only whether the data subject consented to a specific processing purpose, not whether the intended use of the image is consistent with the circumstances of its original capture. To illustrate: a photograph taken at a nationally significant sporting event carries a specific social, historical, and personal meaning, yet the DPA permits that image to be licensed as generic stock content without any obligation to respect or preserve that original context, provided consent for processing was obtained (Data Protection Act, 2019, s. 25). Second, while the DPA's consent framework correctly centers the individual data subject, it approaches that individual's image purely as personal data subject to processing rules, it cannot recognize that the same individual's image may carry their relational identity, historical significance, and personal embeddedness, dimensions of meaning that a standard processing consent neither captures nor protects. The specific proposals for how consent should be reframed, drawing on the French model of contextually anchored, time-limited consent, are developed in Part VI of this paper.

At the regional level, instruments such as the African Union Data Policy Framework (African Union, 2022) and the African Union Convention on Cybersecurity and Personal Data Protection (*Malabo Convention*, 2014) already provide a normative foundation that can be invoked and strengthened without new legislation. The Malabo Convention's definition of personal data covers any information relating to an identified or identifiable natural person, including factors specific to their physical, physiological, mental, economic, cultural, or social identity. This definition is broad enough to encompass images and the fuller dimensions of meaning they carry (*Malabo Convention*, 2014, art. 1). Its consent framework requires that processing be legitimate only where the data subject has given express, unequivocal, free, specific, and informed consent. The conception of data subject rights under the Malabo Convention includes rights of access,

objection, and rectification, and these give individuals meaningful control over how their personal data, including their images, is processed and circulated (*Malabo Convention*, 2014, arts. 1, 13, 16-19). The AU Data Policy Framework reinforces this by recommending that member states develop national personal data protection legislation, establish independent data protection authorities, and ensure that privacy risk mitigation mechanisms are central to national and regional frameworks (African Union, 2022, ss. 5.3.2.4, 5.4.2).

At the international level, the most pressing challenge remains accountability; how does Kenya bind foreign platforms like Getty Images and Alamy that operate beyond its jurisdiction? The GDPR offers an instructive model; its extraterritorial reach applies to any entity processing the data of EU residents regardless of where that entity is located (*General Data Protection Regulation*, 2016/679, art. 3). A similar principle, embedded in Kenya's domestic law and reinforced through continental coordination, could establish that platforms processing the images of Kenyan subjects are subject to Kenyan and African norms regardless of where they are incorporated. It must be acknowledged, however, that the GDPR's extraterritorial effectiveness derives significantly from the EU's considerable market influence and institutional capacity. This is a leverage that Kenya, acting alone, does not currently possess (Couldry & Mejias, 2019). Addressing this constraint realistically requires a combination of approaches: continental coordination through existing regional instruments to build collective regulatory weight; platform accountability agreements that establish minimum standards for consent, attribution, and benefit-sharing without requiring direct extraterritorial enforcement; and the strategic use of reputational and market pressure, given that global platforms operating in African markets have commercial incentives to demonstrate responsible data governance. These are not presented as complete solutions but as realistic and progressive pathways through which meaningful accountability can be built

over time, the specifics of which the following section develops.

These three levels; national reinterpretation, regional coordination, and international jurisdictional reach, form the integrated framework this paper proposes. By embedding these principles into legal and institutional practice, Kenya can begin to redress structural inequities and reclaim agency over both the economic and interpretive dimensions of its imagery, ensuring that the individual whose image circulates in global markets retains meaningful authority over how the relational identity, historical significance and personal embeddedness in their images are represented, circulated, and valued. In doing so, Kenya does not merely address a domestic legal gap, it contributes to a broader continental conversation about how African states can assert sovereignty over their citizens' digital representations in a global landscape that has historically treated African images as extractable commodities.

VI. RECOMMENDATIONS

The preceding analysis has established that Kenya's image-rights challenge is both legal and structural, rooted in a conceptual misalignment between the lived meaning of images and the legal categories available to govern them, and compounded by global digital infrastructures that extract and monetize African images while leaving those depicted without voice, recourse, or benefit.

As discussed throughout the paper, existing frameworks offer partial but insufficient responses. The DPA, 2019, while protecting individual consent and processing rights, cannot capture the fuller dimension of harm to the individual whose image carries relational identity, historical significance, and personal embeddedness (Data Protection Act, 2019). The Copyright Act, 2001 compounds this gap by protecting the photographer as creator while affording no rights to the subject depicted (Copyright Act, 2001, s. 32). Constitutional provisions on dignity, privacy,

and property, though conceptually relevant, have been applied sporadically and without producing a coherent doctrine (Constitution of Kenya, 2010, arts. 28, 31, 40). At the continental level, the Malabo Convention provides a useful normative foundation but requires recalibration to embed African conceptions of personhood and address enforcement gaps against foreign platforms, a recalibration this section proposes (Malabo Convention, 2014). Together, these frameworks leave three specific gaps that the proposals below seek to fill: the absence of recognition of the fuller dimension of individual harm in consent frameworks; the lack of legal recognition of images as carriers of personal narrative and relational significance; and the absence of meaningful cross-border accountability for foreign platforms.

The proposals that follow are presented as a principled and coherent framework for reform, but they are not a fully operational blueprint that can be implemented overnight. Some, particularly at the national level, can be initiated in the near term through targeted statutory amendments and judicial reinterpretation of existing provisions. Others, particularly at the continental and international levels, are medium to long-term objectives that require progressive ratification, institutional capacity-building, and coordinated political will across African states. This paper's contribution is to establish the normative and legal foundation within which these steps can be taken, arguing that the direction of reform is clear even where the pace of implementation will necessarily be gradual.

This final section therefore turns from diagnosis to direction. It outlines a principled path for reform grounded in the conceptual framework laid out in this paper and proposes a structure for a coherent image-rights framework at both the national and continental levels. The aim is not to replicate foreign models, but to build a legal architecture suited to the digital realities that shape how African images are used and governed.

A. Integrating African Personhood into Kenyan Law

Unlike other forms of personal data, images are not neutral objects; they encapsulate personal histories, relational contexts, and social meaning, and their misuse therefore affects not only privacy but also identity, memory, and dignity (Birhane, 2023; Couldry & Mejias, 2019). The law must therefore move beyond narrow privacy protections and adopt a framework that reflects how images function within African societies, recognizing that individuals are both relationally embedded and autonomously constituted, and that their images are inseparable from this dual identity (Kahaka & Maundeni, 2022; Menkiti, 1984). At the national level, this requires three targeted interventions within Kenya's existing legal architecture, interventions that do not create new law but reinterpret and extend what already exists.

Firstly, legislation should codify a guiding principle grounded in African relational personhood, explicitly stating that the use of a person's image shall recognize and protect the individual as both an autonomous and relational being, and that any engagement with an image must safeguard the integrity of this personhood while upholding the inherent dignity that flows from it. This principle is not found in any existing Kenyan statute. Neither the DPA nor the Copyright Act articulates image use through a relational lens grounded in African personhood, and its codification would provide courts with a normative benchmark that current law does not offer (*Data Protection Act*, 2019; *Copyright Act*, 2001; *Constitution of Kenya*, 2010). In the near term, and pending formal codification, courts can begin developing this principle through purposive constitutional interpretation, reading Articles 28, 31, and 40 conjunctively in image disputes to give effect to the relational dimension of personhood even before Parliament formally enacts it as a statutory provision (*Constitution of Kenya*, 2010, arts. 28, 31, 40). The ODPC can similarly issue guidance notes articulating the relational personhood principle in image contexts, providing immediate regulatory direction within its existing mandate (*Data Protection Act*, 2019).

Secondly, consent mechanisms must be extended beyond what the DPA currently provides. While the DPA correctly centers the individual data subject, it approaches their image purely as personal data subject to processing rules, asking only whether consent was obtained for a stated purpose, without recognizing that the individual's image may carry their relational identity, historical significance, and personal embeddedness. The DPA already establishes that consent must be free, specific, informed, and unambiguous which is a solid foundation (Data Protection Act, 2019, ss. 25, 32). However, the DPA's consent standard is transactional and forward-looking; it asks whether the individual agreed to a specific processing purpose, but it does not ask whether the intended use of the image is consistent with the context in which it was originally created. These dimensions of meaning go beyond what a standard processing consent was designed to protect. An individual whose image captures a moment of national sporting significance, a cultural ceremony, or a personal milestone has interests in how that image is used that extend beyond the question of whether processing was consented to. These are interests in narrative authority, in the integrity of how they are represented, and in ensuring that the context from which their image emerged is not erased in favor of commercial utility. A photographer can obtain consent for processing and then license the image as generic stock content without any legal obligation to account for what the image represents.

This paper therefore proposes that the consent framework be extended to explicitly recognize these dimensions by enriching the understanding of what harm to the individual actually means when their image carries this fuller significance. The proposed framework differs from the existing consent standard in two specific ways. First, it introduces contextual boundedness: consent must address not only the processing purpose but also the integrity of representation and the consistency of intended use with the original context of capture. In practical terms, this means that where an image carries personal, historical, or

cultural significance to the individual depicted, consent should address not only the processing purpose but also the integrity of representation and the consistency of intended use with the original context of capture (Menkiti, 1984; Kahaka & Maundeni, 2022). Second, drawing on the French model, consent should be time-limited and specific, ensuring individuals retain ongoing control rather than surrendering their image permanently through a one-time consent, detailing the scope, territorial coverage, duration, and purposes of use, with the requirement that permitted uses remain consistent with the context in which the image was originally created (Ann Fitzgerald, 2019). These are elements the DPA does not currently require for image licensing specifically, and their introduction would represent a targeted and legally precise extension of the existing consent framework (Data Protection Act, 2019).

Moreover, legal definitions should be amended to explicitly incorporate personhood into the existing statutory framework. The DPA currently defines personal data as 'any information relating to an identified or identifiable natural person', with photographs captured within that definition purely as data points (*Data Protection Act*, 2019, s. 2). The Copyright Act, meanwhile, defines a photograph as an artistic work, recognising the creator's rights without any reference to the subject depicted (*Copyright Act*, 2001, s. 2). Neither definition recognizes the narrative, identity, or relational significance an image carries. This paper proposes targeted amendments to both definitions to extend - not replace - their existing scope.

Under the DPA, section 2 should be amended to provide that where personal data takes the form of a person's image, it shall be recognized as inseparable from that person's identity, personal history, narrative, and relational embeddedness, and shall be treated accordingly in any collection, processing, storage, or commercial use. Under the Copyright Act, section 2 should be extended to provide that where a photograph depicts an identifiable person, the subject's personhood interest shall be recognized

alongside the creator's rights in any commercial exploitation of that work. Together these amendments would enrich the legal understanding of what an image is, moving beyond the narrow categorization of images as either personal data or creative property, to recognize that an individual's image carries their relational identity, historical significance, and personal embeddedness, a genuinely novel legal recognition that existing Kenyan law does not provide (Kahaka & Maundeni, 2022; Menkiti, 1984).

Critically, this definition is not a blanket elevation of every photograph to a protected category. It is contextually calibrated. A personhood interest in an image would be engaged where the image was captured in a personal, cultural, or historically significant context, or where its commercial use distorts, commodifies, or misrepresents the subject's identity, narrative, or relational embeddedness. Determining whether these thresholds are met is a matter for the individual depicted, who is best placed to assert their own personhood interest, and for courts and the ODPC applying the following factors: the circumstances and context of original capture; the nature of the event or moment depicted; the individual's own assertion of personal, historical, or cultural significance; and the relationship between the intended commercial use and the original context of capture. These factors are non-exhaustive and should be applied flexibly, giving courts and the ODPC the discretion to recognize the fuller dimension of individual harm in each case. The ODPC is the appropriate regulatory authority for these determinations, not because a new authority is being created, but because this role represents a targeted extension of its existing mandate under the DPA, consistent with the paper's overall reinterpretation approach (*Data Protection Act*, 2019). This threshold enriches the legal question in image disputes, going beyond whether consent was obtained or who owns the copyright, to whether the use of this image respects the personhood of the individual depicted, ensuring that the elevated standard of accountability is applied with precision and giving courts a workable framework for calibrating the person-

hood interest against competing considerations such as freedom of expression, public interest, and legitimate commercial use (*Constitution of Kenya*, 2010, arts. 28, 31, 33). Such an approach also creates the interpretive space necessary for courts to recognize emotional, cultural, and symbolic harms; forms of injury that fall outside traditional intellectual property or privacy categories but are central to understanding how images shape and reflect personhood (Birhane, 2023; Milan & Treré, 2019; Couldry & Mejias, 2019).

Taken together, the three proposals advanced in this section; a guiding principle grounded in African relational personhood, an extended consent framework that recognizes the fuller dimension of individual harm and amended legal definitions that recognize images as expressions of personhood rather than neutral data points, form a coherent and integrated approach to reforming Kenya's image rights landscape within existing legal frameworks. Embedding these protections in law speaks to the wider socio-legal consequences of image exploitation. When images circulate without recognition of the personal and relational identities they express, visibility can mask a profound loss of agency (Birhane, 2023). The repeated international circulation of my father's photographs illustrates this tension, the images travelled widely, but the narrative attached to them slipped increasingly out of his hands. Without legal recognition of the African blended view of personhood, courts lack the tools to assess the deeper harms that arise when images are used in ways that unsettle that balance. By grounding legal protection in this blended view of personhood, while affirming the dignity that flows from it, the law acknowledges that images carry lived meaning, personal history, and social significance, ensuring that individuals retain moral and legal authority over how their likenesses are circulated and their stories told.

B. Reconceptualizing Image Ownership and Benefit Sharing

Current intellectual property frameworks treat images as intangible property belonging to their creators, affording the subject no ownership interest in their likeness (*Copyright Act*, 2001, ss. 2, 22). Complementing the personhood and consent proposals in Part VI, Section A, this subsection addresses the property dimension of the national framework, proposing two extensions to existing IP law that together ensure subjects retain both moral and economic interests in the commercial use of their images.

First, legislation should introduce a personhood and narrative significance clause through targeted amendment to both the Copyright Act and the Data Protection Act. Moral rights are, by design, a category international copyright law leaves largely to national legislatures to define.[2] It is within this latitude that the moral rights of a creator recognized under section 32 of the Copyright Act should be extended to recognize that where a photograph depicts an identifiable person, the subject holds a parallel moral interest in how their image is commercially exploited, grounded not in creative authorship but in personhood (Copyright Act, 2001, s. 32; Kahaka & Maundeni, 2022). Under the DPA, the processing obligations in sections 25 and 32 should be extended to require that any commercial use of an image respect the subject's narrative integrity and identity, going beyond the current requirement of lawful processing to require ethically grounded engagement with the personhood embedded in the image (Data Protection Act, 2019, ss. 25, 32). Together, these amendments would transform image licensing from a purely transactional exercise into an ethically guided process, providing a legal basis for subjects to assert interests in how their likeness is commercially exploited, an interest current law does not recognize (Birhane, 2023; Couldry & Mejias, 2019).

[2] The Berne Convention protects moral rights under Article 6bis. When the TRIPS Agreement later incorporated Berne's substantive provisions, it expressly excluded Article 6bis from that incorporation, leaving the scope of moral rights protection to domestic law (TRIPS Agreement, 1994, art. 9; Berne Convention, 1886, art. 6bis).

Second, legislation should codify a requirement for fair benefit-sharing when images are licensed or sold commercially, enforceable by both regulators and courts. Unlike the moral rights extension above, this proposal does not touch authorship or creative rights; it governs the distribution of commercial proceeds once a license or sale has occurred, a matter international copyright instruments do not address, leaving it open to domestic regulation.[3] Specifically, the Copyright Act should be amended to include a provision stating that where a photograph depicting an identifiable person is licensed or sold for commercial purposes, the subject of that image shall be entitled to fair and equitable remuneration, determined by mutual agreement between the parties, and inclusive of both monetary and non-monetary benefits where appropriate (Copyright Act, 2001, s. 32). Where no agreement is reached, Kenya's courts retain jurisdiction to determine appropriate remuneration through existing civil and constitutional litigation pathways. However, this paper recommends that, as part of the broader legislative reforms proposed here, Parliament consider either expanding the ODPC's mandate to include adjudication of image-related commercial disputes or establishing a dedicated personality rights tribunal to handle the full range of such claims—an institutional development this paper recommends as part of the progressive legislative reforms proposed herein.

This proposal is grounded in a principle that African IP law has already recognized (in a related context): that where traditional knowledge or cultural expressions are commercially exploited, the communities and individuals whose heritage, identity, or knowledge is embedded in that expression are entitled to share equitably in the value generated (Swakopmund Protocol, Sections 9.1 and 9.3). This principle has been operationalized in the context of traditional knowledge and expressions of folklore, demonstrating that benefit-sharing within an African IP frame-

[3] Berne and TRIPS are concerned with the rights of authors and creators rather than the allocation of licensing revenue between parties (WIPO, 2024).

work is not a novel or untested concept but one that Africa's own legal tradition has already embraced. The clearest regional articulation of this principle is found in the Swakopmund Protocol on the Protection of Traditional Knowledge and Expressions of Folklore (ARIPO, 2010, as amended 2019), which, while not binding on Kenya as a non-party, provides directly relevant and persuasive precedent from within Africa's legal tradition. Section 9 of the Protocol requires fair and equitable sharing of benefits arising from the commercial or industrial use of traditional knowledge, determined by mutual agreement and inclusive of non-monetary benefits such as community development (Swakopmund Protocol, 2019, s. 9). More significantly for this paper, Section 19 protects expressions of folklore, defined to include visual cultural expressions, against reproduction, publication, adaptation, and fixation, with the Protocol explicitly providing that fixation includes still photography and requiring free and prior informed consent for any such use (Swakopmund Protocol, 2019, s. 19). This makes the Swakopmund Protocol the closest existing African instrument to a regional image rights framework, one that already recognizes the requirement of consent for commercial photography and the entitlement to benefit-sharing where commercial gain is involved.

Kenya's Protection of Traditional Knowledge and Cultural Expressions Act, 2016, already recognizes benefit-sharing within the domestic IP framework, albeit limited to traditional communities and cultural expressions (*Protection of Traditional Knowledge and Cultural Expressions Act, 2016). Extending this principle to ordinary image contexts is therefore not a novel departure but a logical progression of an approach Kenya has already embraced.* Where an image embodies an individual's identity, narrative, and relational embeddedness, whether or not it falls within the technical definition of traditional knowledge or folklore, that individual should share equitably in the commercial value generated from it, with provisions for collective benefit where the image carries cultural or historical significance beyond the

individual depicted (Kahaka & Maundeni, 2022; Ijuo, 2025; Swakopmund Protocol, 2019, s. 9). This extension fills the precise gap that the Swakopmund Protocol itself does not cover; the commercial use of images of ordinary individuals whose likenesses are extracted and monetized through global stock photography platforms without consent or compensation.

Taken together, the two proposals in this section, a personhood and narrative significance clause that recognizes the subject's moral interest in their image alongside the creator's rights, and a codified benefit-sharing requirement grounded in African IP precedent, directly address the structural imbalance in current global image markets. By embedding both ethical and equitable standards into commercial transactions involving African images, these proposals correct a disparity that existing IP frameworks were never designed to address, ensuring that the commercial value generated from African images flows not only to platforms and photographers but also to the individuals whose images carry relational, historical, and personal significance. At the continental level, the Swakopmund Protocol provides a model that the AU could adopt more broadly through the Malabo Convention recalibration proposed in Part VI, Section C, extending benefit-sharing and consent requirements for image use across all African states regardless of their membership of ARIPO.

C. Strengthening Continental and International Frameworks for Image Rights Protection

The national reforms proposed in Sections A and B of Part VI while necessary, are insufficient on their own as the extraction and commercial exploitation of African images is fundamentally a cross-border phenomenon, driven by platforms headquartered in the Global North, operating beyond the reach of Kenyan domestic law, and enabled by international digital infrastructures that existing national frameworks cannot adequately address (Couldry & Mejias, 2019; Birhane, 2023). Addressing this reality

requires action at both the continental and international levels, and this paper advances three proposals for doing so.

The Malabo Convention should be recalibrated to embed the blended personhood framework developed in this paper, recognizing both the relational and autonomous dimensions of the individual, ensuring that image rights protections reflect Africa's distinct philosophical and cultural context rather than reproducing imported Western categories. This recalibration would involve defining a person's image as inseparable from their identity and life story, mandating informed and contextually bounded consent that recognizes the fuller dimension of individual harm, and establishing mechanisms for equitable benefit-sharing across borders (*Malabo Convention*, 2014). Such recalibration does not require a new continental instrument; it requires purposive interpretation and amendment of an existing one, consistent with this paper's overall reinterpretation approach. The Swakopmund Protocol's existing benefit-sharing and consent framework for traditional knowledge and expressions of folklore, including its explicit recognition of still photography as an act requiring free and prior informed consent, provides a model that the AU could incorporate into the Malabo Convention's architecture, extending these protections beyond traditional and folkloric expressions to all image contexts involving identifiable African persons (*Swakopmund Protocol*, 2019, ss. 9, 19). It must be acknowledged, however, that the Malabo Convention's practical reach is currently limited; it has been ratified by only a small number of African states, and its enforcement mechanisms remain underdeveloped (*Malabo Convention*, 2014). This proposal is therefore a medium- to long-term normative objective, the immediate value of which lies in establishing the philosophical and legal framework within which African states can progressively align their domestic laws, rather than a mechanism that can be operationalized immediately.

Secondly, continental dispute resolution mechanisms should be strengthened to allow African subjects to seek redress when

images are exploited without consent or fair benefit by foreign platforms. Existing mechanisms, including the ODPC at the national level and the African Court on Human and Peoples' Rights at the continental level, provide a foundation but do not currently extend to cross-border image licensing disputes involving foreign commercial platforms (*Data Protection Act*, 2019; African Court on Human and Peoples' Rights, 1998). This paper proposes that the Malabo Convention's enforcement framework be extended to explicitly cover such disputes, drawing on the GDPR's extraterritorial jurisdiction model, which applies to any entity processing the data of individuals within its territorial scope regardless of where that entity is incorporated, as a precedent for establishing that platforms processing the images of African subjects are subject to African norms and enforcement mechanisms (*General Data Protection Regulation*, 2016/679, art. 3). It must be acknowledged that the GDPR's extraterritorial reach derives in significant part from the EU's economic and political leverage over major platforms, leverage that Kenya and the AU do not currently possess to the same degree (Couldry & Mejias, 2019). Nevertheless, the jurisdictional principle itself is sound and transferable; to the extent that African states collectively strengthen their regulatory frameworks and coordinate through continental instruments such as the Malabo Convention, the practical enforceability of extraterritorial claims becomes progressively more viable; a conditional outcome that depends on political will and institutional coordination rather than economic scale alone (*Malabo Convention*, 2014). In the near term, this proposal's most realistic application lies in Kenya legislating domestically to establish that platforms processing the images of Kenyan subjects, regardless of where those platforms are incorporated, are subject to Kenyan image rights norms, while simultaneously building the continental coordination through the Malabo Convention and AU Data Policy Framework necessary for broader regional enforcement over time.

Furthermore, this paper proposes a platform accountability framework as a targeted mechanism for ensuring that foreign

platforms operating in African markets are bound by minimum standards for consent, attribution, and benefit-sharing when licensing African images. This framework would require major stock photography platforms to enter into bilateral or multilateral agreements with designated national authorities*, whether through an expanded ODPC mandate or a dedicated regulatory body established for this purpose,* modeled on the data transfer agreements used under the GDPR's adequacy framework (*General Data Protection Regulation*, 2016/679, arts. 45-46). Such agreements would require platforms to obtain contextually bound consent consistent with the standards proposed in Section A above and ensure fair and equitable benefit-sharing consistent with the framework proposed in Section B as above. It must be acknowledged that African states currently lack the economic and political leverage that underpins the West's (particularly the EU's) ability to compel platform compliance, a limitation this paper does not dismiss. However, platform accountability agreements are meaningfully different from pure extraterritorial enforcement; they are negotiated rather than imposed, and platforms have commercial incentives to enter into them in exchange for regulatory certainty and continued market access in African markets, which represent a significant and growing share of global digital consumption. African states can progressively build this leverage through continental coordination and regulatory coherence. This approach does not require new international treaties or enforcement bodies; it works through bilateral negotiated agreements modeled on frameworks that already exist in international data governance practice, making it immediately actionable within the current regulatory landscape (*General Data Protection Regulation*, 2016/679, arts. 45-46).

By linking these protections to continental instruments and existing jurisdictional principles, African states can collectively enhance sovereignty over digital representations of their citizens, mitigate exploitative practices by foreign platforms, and establish a pan-African standard for image ethics and rights that respects the narrative and historical dimensions of images (Mi-

lan & Treré, 2019; Birhane, 2023). Ultimately, the integration of national and continental frameworks ensures that African individuals can exercise meaningful control over their visual heritage, supported by institutional frameworks that give that control legal force, aligning ethical and commercial practices with African values and maintaining compliance with international data governance obligations, all while affirming the primacy of personhood, dignity, and narrative integrity (Couldry & Mejias, 2019; Kahaka & Maundeni, 2022).

VII. CONCLUSION

The circulation of African images in global digital markets exposes a persistent tension between visibility and agency, rooted in historical patterns of extraction and reinforced by contemporary legal gaps. Prevailing frameworks, grounded in privacy, intellectual property, or data protection, remain inadequate because they fail to recognize the personal, historical, and relational significance that images hold for the individuals depicted. What is needed is not merely a refinement of existing tools, but a reorientation of legal reasoning toward an account of African personhood that captures both autonomy and relational embeddedness, one that sees the individual not as an isolated rights-holder but as a person whose image carries their relational identity, historical significance, and personal embeddedness within family, community, and cultural memory.

Drawing on the blended model articulated by contemporary African authors, this paper shows that African philosophical traditions already provide the conceptual resources to recognize individuals as simultaneously autonomous and socially embedded. This dual perspective clarifies why images matter beyond their commercial value, why their misuse causes harm that extends beyond narrow legal categories to encompass the individual's relational identity, historical significance, and personal embeddedness, and why legal frameworks must account for these dimen-

sions—dimensions that existing Kenyan law, modeled largely on Western individualistic frameworks, does not currently reach.

Building on this foundation, the recommendations proposed in this paper offer a practical pathway for translating theory into law, operating at three levels simultaneously. At the national level, targeted amendments to the Data Protection Act and the Copyright Act—introducing a guiding principle grounded in African relational personhood, extending consent frameworks to recognize the fuller dimension of individual harm, and redefining images as inseparable from the personhood of those depicted—would shift the fundamental legal question in image disputes from whether consent was obtained or who owns the copyright, to whether the use of an image respects the personhood of the individual it represents. At the continental level, the recalibration of the Malabo Convention to embed African conceptions of personhood and the strengthening of dispute resolution mechanisms would enable African subjects to assert interests against foreign platforms across borders. At the international level, a platform accountability framework modeled on the GDPR's adequacy mechanisms would require major stock photography platforms operating in African markets to meet minimum standards for consent, attribution, and benefit-sharing, ensuring that the commercial value generated from African images flows not only to platforms and photographers but also to the individuals whose images carry relational, historical, and personal significance.

These proposals do not seek to replace existing frameworks, they seek to reinterpret and extend them through an African philosophical lens, ensuring that legal reform is both practically achievable and normatively grounded in African lived realities. The goal is not to close Kenya off from global image markets but to ensure that African subjects participate in those markets as full agents retaining meaningful control over their images, sharing equitably in the value they generate, and asserting the narrative authority that has too long been denied to them.

Ultimately, this paper argues for a jurisprudence that recog-

nizes African individuals as full subjects, bearing personal identity, relational significance, and historical presence. Grounding image rights in an African account of personhood allows the law to reclaim narrative authority, redress asymmetries in global representation, and uphold dignity in a manner that reflects the lived realities of African individuals and the communities within which their identities are formed. Such a framework positions African societies not as passive objects of global image economies, but as active agents shaping the ethical, cultural, and legal terms under which their likenesses circulate; asserting, in the digital age, the same sovereignty over their stories and identities that data colonialism has for too long sought to deny.

REFERENCES

African Court on Human and Peoples' Rights. (1998). *Protocol to the African Charter on Human and Peoples' Rights on the Establishment of an African Court on Human and Peoples' Rights. African Union.*

African Regional Intellectual Property Organization. (2010, as amended 2019). *Swakopmund Protocol on the Protection of Traditional Knowledge and Expressions of Folklore*. ARIPO

African Union. (2022). African Union data policy framework. African Union Commission.

Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C. World Trade Organization.

Alamy. (2023). Contributor terms and conditions. https://www.alamy.com/terms/contributor/

Alamy. (2024). Editorial content licensing.

Amodu, S.A & F. Mohammed (2022). *The Conception of Personhood and Community in Africa*. Enyojo Journal of Philosophy and Humanities, 97-109.

Ann Njoki Kumena v. KTDA Agency Ltd. [2019]. *eKLR*.

Bayuo, J. (2025). Personhood and community: African philosophical perspectives. Nursing Philosophy, 26, 1-11.

Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, as revised at Paris, July 24, 1971. World Intellectual Property Organization.

Birhane (2023). Algorithmic colonization of Africa. In *Imagining AI: How the World Sees Intelligent Machines* (pp. 247-260). Oxford University Press. https://doi.org/10.1093/oso/9780192865366.003.0016

Bowmans. (2018). The interplay among rights: Copyright, image rights and the right to privacy. https://bowmanslaw.com/insights/the-interplay-among-rights-copyright-image-rights-and-the-right-to-privacy/

Brindle, M., & Florman, N. (2021). The Maasai Intellectual Property Initiative: A 20th-century model for turning assets into income. *Journal of Fair Trade, Volume 2, Issue 2*, 5-12. https://www.researchgate.net/publication/352677340_The_Maasai_Intellectual_Property_Initiative_a_20th-century_model_for_turning_assets_into_income

Brindle, M., & Layton, R. (2017). Social entrepreneurship for development: A business model. Routledge.

Burchell, J. M. (1998). *Personality rights and freedom of expression: The modern actio iniuriarum*. Juta.

Case Western Reserve University Law Library. (n.d.). *Personality rights*. https://lawresearchguides.cwru.edu/IP/personality-rights

Chanock, M. (1986). *Law, custom and social order: The colonial experience in Malawi and Zambia.* Cambridge University Press.

Charter of Fundamental Rights of the European Union. (2000). *Official Journal of the European Communities C364*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P/TXT

CIPIT. (n.d.). *Legal protections for image rights in Kenya*. Strathmore University. https://cipit.strathmore.edu/legal-protections-for-image-rights-in-kenya/

Code civil [French Civil Code] art. 9 (1804). https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070721/

Constitution of the Republic of Kenya, 2010.

Constitution of the Republic of South Africa, 1996. https://www.gov.za/documents/constitution-republic-south-africa-1996

Copyright Act, Cap. 130 (Kenya).

Couldry, N., & Mejias, U. A. (2019). Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media*, *20*(4), 336-349. https://journals.sagepub.com/doi/10.1177/1527476418796632

Data Protection Act 2019 (Kenya).

Dwivedi, A. V. (2024). Individualism. In *EBSCO Research Starters: Literature and Writing*. https://www.ebsco.com/research-starters/literature-and-writing/individualism

European Data Protection Board. (2020). *Guidelines 05/2020 on consent under Regulation 2016/679*.

Fitzgerald, A. (2019, November 26). *Images rights in France (Droit à l'Image)*. https://www.annfitzgeraldfixer.com/post/2019/11/26/images-rights-in-france-droit-%C3%A0-limage

General Data Protection Regulation, Regulation (EU) 2016/679 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Getty Images & Agence France-Presse. (2026, January 14). *Getty Images and Agence France-Presse sign multi-year renewal of longstanding global content partnership* [Press release]. https://newsroom.gettyimages.com

Getty Images. (2024a). *Work with us: Royalty rate card*. https://www.gettyimages.com/workwithus

Getty Images. (2024b). *Rights and clearance: Editorial content*. https://www.gettyimages.com/rights-and-clearance

Getty Images. (n.d.). *Getty Images contributor agreement v5.1: Fact sheet*. https://contributors.gettyimages.com/article/5610

Gyekye. K.(1995). *African Philosophy in Search of Identity,* Africa Today Associates publication.

Hodgson, D. L. (2011). *Being Maasai, Becoming Indigenous: Postcolonial Politics in a Neoliberal World*. Indiana University Press.

Honoré A.M. (1961). Ownership. *The Nature of Property and the Value of Justice*, 370-375.

Ijuo, I. (2025). Data colonialism and information revolution: Rethinking consent in the age of big data. ResearchGate.

Jessicar Clarise Wanjiru v. Davinci Aesthetics & Reconstruction Centre & 2 Others [2017] eKLR.

Kahaka, M., & Maundeni, W. (2022). Comparing some traditional Western and African conceptions of personhood. *European Journal of Humanities and Social Sciences*, *2*(5), 57-62.

Kariuki, F. (2016). Property law. Strathmore University Press.

Knowledge Commons Brasil. (n.d.) Digital colonialism & the Internet as a tool of cultural hegemony.

Kwet, M. (2019). Digital colonialism is threatening the Global South. A*l Jazeera - Opinion: Science & Technology*.

Mamdani, M. (1996) Citizen and Subject: Contemporary Africa and the Legacy of Late Colonialism. *Princeton University Press*, Princeton.

Mbiti, J. S, (1969). African Religions and Philosophy (second revised and enlarged edition). Oxford: Heinemann Publishers.

Menkiti, I. A, (1984). Person and community in African traditional thought in R.A Wright (Ed.), *African Philosophy: An Introduction* (p. 171-181). Washington: University Press of America.

Meyer v. Nebraska, 262 U.S. 390 (1923).

Milan, S., & Treré, E. (2019). Big Data from the South(s): Beyond Data Universalism. *Television & New Media*, 20(4), 319-335. https://journals.sagepub.com/doi/10.1177/1527476419837739

MultiChoice (T) Ltd v Three Elite Athletes (Civil Case No. 15 of 2021) [2023] High Court of Tanzania (Commercial Division).

Neethling, J. (2005**).** Personality rights: A comparative overview. *The Comparative and International Law Journal of Southern Africa, 38*(2), 210-245.

Nwokedi, C. (2021). Copyright in photographs and image rights in Nigeria: Banire v NTA-Star TV Network Ltd as a case study. Academia.edu. https://www.academia.edu/53370837

Pierce v. Society of Sisters, 268 U.S. 510 (1925).

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383-423.

Protection of Traditional Knowledge and Cultural Expressions Act*, Cap.218A.*

Samuel D. Warren & Louis D. Brandeis. (1890). *The Right to Privacy*, 4 Harv. L. Rev. 193, 213.

Synodinou, T. (2014). Image right and copyright law in Europe: Divergences and convergences. *SSRN,* 181 - 207.

T.O.S. v. Maseno University & 3 Others [2016] eKLR.

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A practical guide. Springer.

Waldron, J. (2010). Property law. In D. Patterson (Ed.), A companion to philosophy of law and legal theory (2nd ed., pp. 107-122). Blackwell Publishing.

Wanjiru v Machakos University [2022]. ekLR.

Wilkinson, J.R. (2002). South African Women and the Ties that Bind in P.H. Coetzee & A.P.J. Roux, (Eds.), *Philosophy from Africa: A text with readings.* (pp.343-360). Cape Town: Oxford University Press.

World Intellectual Property Organization. (2024). Summary of the Berne Convention for the Protection of Literary and Artistic Works. https://www.wipo.int/en/web/treaties/ip/berne/summary_berne

JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 6, Issue 1 (2026) p.169-262
https:doi.org/10.52907/jipit.2026.617

Governing AI-Generated Likeness: African Legal and Philosophical Frameworks

*Onyinyechi Cynthia Igodo**

ABSTRACT

The governance of likeness remains fragmented in Africa, with legal protections scattered across privacy, dignity, defamation, data protection, and copyright doctrines. Unlike the United States, where publicity rights provide a mechanism for protecting the commercial value of individual likeness, many African jurisdictions lack a comprehensive framework governing the capture, use, and exploitation of likeness. This challenge is further complicated by African conceptions of identity, in which likeness may signify not only individual identity but also communal dignity, cultural heritage, spirituality, and collective identity. Consequently, debates on image rights in Africa implicate two overlapping but distinct categories: individual likeness rights and communal cultural imagery. Artificial intelligence (AI) intensifies these challenges. Generative AI systems, capable of producing hyper-realistic deepfakes, facilitate the unauthorized replication and commercial exploitation of individual likenesses while also enabling the extraction, manipulation, and commodification of communal cultural imagery without consent, attribution, or benefit-sharing. Existing legal regimes in many African jurisdictions are ill-equipped to address these harms, particularly where AI-generated representations combine identifiable persons with culturally significant imagery. Through a comparative analysis of South Africa, Nigeria, and Kenya, this paper examines how African legal systems regulate individuals' likeness rights and communal cultural imagery within constitutional, intellectual property, privacy, and technology governance frameworks. It argues that existing privacy-based and copyright-based protections are inadequate to address AI-driven likeness replication and cultural appropriation. Drawing on Ubuntu and broader African philosophies of relational personhood, this paper proposes a hybrid governance framework that distinguishes between individual image rights and interests in communal cultural imagery while recognizing their intersection. It

* LL. B (EBSU), LL.M(QMUL), MIP (Africa University). Principal Associate at CLP Legal, Lagos, Nigeria.

advocates a context-sensitive, decolonial approach to AI governance that integrates personality rights, cultural heritage protection, collective consent mechanisms, indigenous data sovereignty, and communal custodianship to safeguard likeness in Africa's digital future.

Keywords: African Philosophy (Ubuntu), Artificial Intelligence, Image Rights and Cultural Heritage, Intellectual Property Law, Privacy and Publicity Rights

TABLE OF CONTENTS

ABSTRACT 169

I. INTRODUCTION 172

II. CONCEPTUAL AND PHILOSOPHICAL FRAMEWORKS 179

- *A. Image Rights: Concepts, Legal Doctrines, and Cross-Jurisdictional Perspectives* 179
- *B. African Philosophies: Relational Identity and Communal Cultural Imagery* 182
- *C. From Relational Identity to Digital Futures* 187
- *D. Communal Cultural Imagery and Traditional Cultural Expressions* 192
- *E. Contemporary Relevance of Communal Cultural Imagery and Legal Foundations* 195

III. LEGAL FRAMEWORKS FOR IMAGE RIGHTS AND RIGHTS IN COMMUNAL CULTURAL IMAGERY IN AFRICA 196

- *A. Image Rights as Constitutional Dignity and Privacy Interests* 197
- *B. Individual Image Rights Through Data Protection and Digital Privacy Frameworks* 204
- *C. Intellectual Property Law and the Protection of Likeness* 206
- *D. Limits of Existing Intellectual Property and Individual Image-Rights Frameworks* 210

E. Statutory Law Remedies for Digital and AI-Enabled Harms 213
F. AI, Deepfakes, and Emerging Regulatory Responses 214
G. The Limits of Existing Frameworks in the Age of AI 215

IV. AI AND THE DISRUPTION OF LEGAL AND ETHICAL FRAMEWORKS 217
A. Consent and Relational Identity 221
B. Authorship, Creativity, and Collective Agency 222
C. Cultural Representation and Collective Identity 224

V. RELATIONAL IMAGE GOVERNANCE AND COMMUNAL CULTURAL PROTECTION 225
A. Indigenous and Comparative Models of Cultural Image Governance 226
B. Ubuntu Relational Personhood and Image Governance 230
C. Governance Principles for Relational Image and Cultural Representation 232
D. Operationalizing Communal Cultural Image Governance in the AI Era 240
E. Continental Coordination and African AI Governance . 244

VI. CONCLUSION 245

REFERENCES 247

I. INTRODUCTION

> 'Under Aboriginal law, the right to create artworks depicting creation and dreaming stories, and to use pre-existing designs and totems of the clan, resides in the traditional owners as custodians of the images. The traditional owners have the collective authority to determine whether these images may be used in an artwork, by whom the artwork may be created, to whom it may be published, and the terms, if any, on which the artwork may be reproduced…
>
> Aboriginal artwork will often depict secret parts of a dream that will only be recognized and understood by those who are initiated into the relevant ceremonies or at least have a close knowledge of the cultural significance of the story. It is therefore important that any reproduction is accurate in every respect and done with full, proper permission of the artist and community to avoid offending the traditional owners.
>
> The traditional owners have the responsibility to take action to maintain the dreaming and to punish those considered responsible for the breach…
>
> The images used by Banduk Marika in *Djanda and the Sacred Waterhole* are associated with her ancestral creation place, Yelangbara. *Her rights to use the image arise by virtue of her membership of the land-owner group in that area.* Although Banduk Marika owns the copyright in the artwork under Australian copyright law, *under Aboriginal law she holds the image on trust for all other Yolngu* who have an interest in the story. *She cannot use an image in such a way as to undermine the rights of her beneficiaries'.* (emphasis added). Aboriginal concepts of ownership of images (Janke, 1995).

In the landmark case of *Milpurrurru v Indofurn Pty Ltd* (1994), a group of Aboriginal artists from Arnhem Land Northern Territory, Australia, brought proceedings against a manufacturer that had reproduced sacred Dreaming designs on carpets sold commercially without their consent. These designs, known as *Madayin miny'tji*, are sacred clan symbols representing ancestral beings, spiritual law, and communal identity. Justice von Doussa held that the unauthorized reproduction caused profound cultural and spiritual harm extending beyond the individual artists to the Yolngu community (Janke, 1995). By recognizing 'cultural insult' as a legally cognizable harm, the Federal Court acknowledged that the unauthorized use of sacred imagery may inflict communal, spiritual, and cultural injury in addition to econom-

ic loss. *Milpurrurru,* therefore, marked a significant moment in intellectual property jurisprudence by demonstrating that those traditional cultural designs, although fixed in works created by individual artists, may simultaneously embody collective heritage, cultural authority, and communal dignity that cannot be adequately protected through conventional intellectual property doctrines alone (Janke, 1995).

The significance of the *Milpurrurru* decision extends beyond Australia because it illustrates a broader governance challenge; culturally significant imagery frequently embodies meanings, obligations, and communal interests that exceed the individualized concepts of ownership and authorship upon which modern intellectual property law is largely founded. Similar tensions have emerged in many parts of the world where Indigenous and traditional communities have sought to resist the commercial appropriation of their collective identities.

One prominent African example concerns the Maasai community of Kenya and Tanzania. In 2012, a group of Maasai elders discovered that over a thousand global companies, including Louis Vuitton, Jaguar Land Rover, and Ralph Lauren, had appropriated the 'Maasai' name, red *shúkà* cloth, and other elements of Maasai cultural identity without authorization or compensation (Afro-IP, 2017; Brindle, & Florman, 2021; Livni, 2016). These appropriations often detached Maasai cultural symbols from their historical and social significance, transforming them into commercial branding assets for global profit in ways the community regarded as exploitative and deeply offensive (Brindle, & Florman, 2021; Maasai Intellectual Property Initiative, n.d). In response to this, the Maasai Intellectual Property Initiative was established to reclaim control over the community's cultural heritage and to challenge the continuing unauthorized commercial exploitation of Maasai identity (Maasai Intellectual Property Initiative, n.d).

The experience of both the Yolngu and Maasai reveals a common legal deficiency. In each instance, what was appropriated

was not merely an aesthetic design or marketable symbol, but a visual manifestation of communal history, spirituality, identity, dignity, and belonging. Their living image, so to speak. Existing intellectual property regimes, with their emphasis on individual ownership, originality, and economic exploitation, struggle to accommodate these collective interests because they are not designed to recognize communities as custodians of living cultural identities. These cases therefore expose a broader normative gap in the governance of culturally significant imagery.

This challenge assumes particular significance within African philosophical traditions, where identity has long been understood as both personal and relational. Across many African societies, personhood is conceived not merely as an individual possession but also as a relational construct grounded in kinship, spirituality, and communal belonging (Gyekye, 1997, pp. 45–46; Lumumba, 2023, pp. 2-3). John Mbiti's (1970) famous maxim, 'I am because we are, and since we are, therefore I am' (p. 141), encapsulates the foundational tenet of African personhood; the self exists through social relationships and moral interdependence, a shared humanity (Gyekye, 1997). This understanding does not erase individual autonomy; rather, it situates individual dignity within a broader communal framework of recognition and responsibility. Consequently, likeness, whether expressed through facial features, traditional attire, bodily markings, ceremonial objects, or ritualistic gestures, may constitute more than an individual's personal attribute. It may also function as a symbol of collective identity, cultural continuity, and cultural dignity. Thus, whereas Western legal traditions often conceptualize likeness as belonging to the 'self', African ontology suggests that aspects of identity may simultaneously belong to the 'we' that shapes, sustains, and gives meaning to the *self* (Menkiti, 1984, pp. 172, 179).

This relational understanding of identity is reflected in cultural practices across the continent. Clan scarification among the Yoruba (Orie, 2011), Igbo (Chisam, 2024), and Dinka (Ahon-

si, 2024); patterned hairstyles of the Himba (Afriklens, 2024; Afriquei Noir Magazine, 2025; Amazing and Wonderful, 2024; McGinty, n.d); and ritualized gestures such as the Luo handshake, Yoruba prostration, Shona clapping (*kuwombera*), and Akan posture of deference, all serve as visual languages of belonging (Kquofi, Amate, & Tabi-Agyei, 2013; Takim & Ozim, 2025). The unauthorized reproduction, manipulation, or distortion of such imagery may therefore implicate not only personal dignity, but also a violation of relational dignity, which is a core principle of African ethics (Mbiti, 1970; Metz, 2011; Segun, 2024).

Despite this rich philosophical grounding, African legal systems remain inadequately equipped to comprehensively regulate either individual image rights or interests in communal cultural imagery (Cornelius, 2008; Ogbah et al., 2024; Ogonjo, 2023). Existing legal frameworks largely reflect inherited European legal traditions that conceptualize likeness through fragmented doctrines of privacy, property, intellectual property and commercial personality, rather than recognizing its communal, cultural and relational dimension (Mangope & Alberts, 2022; Nwauche, 2015). While these approaches provide useful protections in some contexts, they often fail to account for the collective and relational dimensions of identity that characterize many African societies. The dominance of Western models thus leaves limited space for alternative epistemologies that might better respond to the ethical dilemmas of the AI era (OfosuAsare, 2025; Segun, 2024).

Similarly, legal efforts to protect traditional cultural expressions through copyright and folklore frameworks remain limited and frequently vest control in state institutions rather than communities (Fuente, 2003; Nwauche, 2017). As Nwauche (2017) observes, intellectual property frameworks vest negative protection of traditional cultural expressions on communities. This provides them with a veto-based safeguard that prevents unauthorized use of their folklore by requiring third-party consent and benefit-sharing, usually facilitated by state institutions. This vests control of traditional cultural expressions in

governmental bodies rather than in the originating communities (Nwauche, 2017). For example, Nigeria's Copyright Act, 2022 protects expressions of folklore against unauthorized reproduction, adaptation, and public communication, particularly where such use occurs outside customary contexts or for commercial purposes, with limited exceptions for fair dealing, education, illustration, and incidental use. However, enforcement authority largely resides with the Nigerian Copyright Commission rather than directly with the communities themselves (Sections 74(4), 75 and 76 Nigerian Copyright Act, 2022; Oyiwona, 2025). Consequently, these communities remain unable to exercise meaningful control over representations central to their cultural identity.

The rise of generative AI has exacerbated these vulnerabilities. As AI advances, it reshapes how human likeness is captured, reproduced, and circulated across digital environments. These systems trained on vast datasets, containing photographs, artworks, museum collections, online videos, and ethnographic archives, can now generate synthetic faces, voices, attires, gestures, rituals, and artistic styles (Ndubisi, 2024). These outputs, often produced without consent, attribution, or compensation, blur the boundary between authentic and synthetic images and extend historical patterns of appropriation into the algorithmic domain (Birhane, 2020; Salami, 2024; Segun, 2024).

In Africa, the problem is even more complex. AI systems increasingly operate across borders, often extracting data from African populations with weak regulatory environments (Segun, 2024; Salami, 2024). Scholars have described this phenomenon as digital or algorithmic colonization, noting it perpetuates historical patterns of cultural extraction under the guise of innovation (Birhane, 2020; Couldry & Mejias, 2018; 2019).

At the same time, Africa represents a site of normative pluralism and legal innovation (Zeleza, 2024). Across the continent, statutory laws, customary norms, and constitutional principles co-exist and interact dynamically (Kang'ara, 2011; Zeleza, 2024). This plurality reveals the limits of governing likeness solely

through intellectual property or privacy frameworks (Kang'ara, 2011). Communities such as the Maasai and the Yolngu demonstrate the inadequacy of treating likeness as a purely individual or commercial asset. In many African societies, images convey communal memory, collective dignity, and social identity. Its unauthorized appropriation, distortion, or manipulation, therefore, implicates not only personal rights but broader questions of cultural sovereignty and relational personhood. Addressing these challenges requires legal and ethical frameworks that recognize both individual autonomy and the communal dimensions of identity (Kang'ara, 2011). These plural legal traditions provide important normative resources for rethinking the governance of identity in the AI era. African philosophies such as Ubuntu foreground dignity, relationality, reciprocity, and communal responsibility as foundational ethical values capable of informing technology governance beyond purely individualistic frameworks (Kang'ara, 2011; Segun, 2024).

This paper therefore argues that existing privacy, copyright, and publicity-based frameworks are inadequate for addressing the challenges posed by AI-driven image replication. It contends that AI's capacity to reproduce, manipulate, and circulate human likeness exposes the limits of Western, individualistic conceptions of image rights. Through a comparative analysis of South Africa, Nigeria, and Kenya, this paper demonstrates that effective governance of AI-generated representations requires a dual framework capable of protecting both individual image rights and communal cultural imagery while recognizing the intersection between them. These jurisdictions are selected because they exhibit distinct but evolving approaches to privacy, dignity, personality rights, cultural heritage, intellectual property, and digital governance, thereby providing valuable comparative insights into emerging legal responses to synthetic identity technologies (Nkem, 2024). Their relevance therefore offers critical insights for examining how African legal systems are responding to the challenges posed by synthetic identity and the global debates on AI regulation and digital justice.

This paper draws on two intersecting theoretical lenses. First, critical legal pluralism highlights how multiple normative orders shape the governance of likeness, particularly in societies where customary and statutory systems coexist (Kleinhans & Macdonald, 1997, p. 31; Swenson, 2018). Second, African philosophies of personhood, exemplified by Ubuntu, conceptualize identity as socially embedded and relationally constituted (Mbiti, 1970). Together, these frameworks provide the basis for a decolonial approach to AI governance that recognizes both individual autonomy and communal custodianship.

Ultimately, this paper argues that reimagining image rights through African legal and philosophical traditions is not simply a regional response but a global ethical necessity. As generative AI accelerates the production and circulation of synthetic likeness, legal frameworks grounded in dignity, relationality, and collective responsibility may provide critical pathways for governing technological futures in ways that empower, rather than exploit, individuals and communities.

Consequently, this paper proceeds as follows. Part II develops the conceptual framework by distinguishing between individual image rights and communal cultural imagery, contrasting Western individualistic approaches with African relational paradigms. Part III examines the regulation of image rights, cultural heritage, and traditional cultural expressions in Nigeria, Kenya, and South Africa. Part IV analyzes the ways generative AI disrupts both individual likeness protections and communal cultural governance through synthetic cultural imagery and algorithmic appropriation. Part V proposes a hybrid governance framework integrating personality rights, cultural heritage protections, collective consent mechanisms, indigenous data sovereignty principles, and communal custodianship models. Part VI concludes.

II. CONCEPTUAL AND PHILOSOPHICAL FRAMEWORKS

A. Image Rights: Concepts, Legal Doctrines, and Cross-Jurisdictional Perspectives

In legal discourse, likeness refers to any identifiable representation of an individual's physical appearance or personal attributes, including photographs, voice recordings, gestures, signatures, digital avatars, or simulated representations capable of conveying recognition (Ogonjo, 2023). Legal recognition of likeness extends beyond facial appearance to contextual cues such as attire, tattoos, styles, or mannerisms that render a person recognizable (Asia IP, 2023; Guernsey IP, n.d). Image rights therefore concern the protection, control, and authorization of the use of that likeness, particularly in contexts involving publicity, privacy, identity, and commercial exploitation (Edema & Ecoma, 2024; Mostruat & Cruz, 2023). Logeais and Schroeder (1998) define image rights as the exclusive right to one's own image, enabling individuals to prevent unauthorized dissemination or exploitation. The right of publicity, in contrast, primarily addresses the commercial exploitation of persona, while personality rights more broadly recognize social identity as legally significant, encompassing both image and the social expectations tied to conduct and reputation (Edema & Ecoma, 2024; Mostruat & Cruz, 2023).

These rights occupy an increasingly significant position at the intersection of privacy, personality, property, and intellectual property law, safeguarding personal autonomy, dignity, and economic interests against the unauthorized appropriation or exploitation of one's likeness (McCarthy & Schechter, 2023; Mostruat & Cruz, 2023). Consequently, image rights attach to natural persons and focus on the protection of individual recognition and persona.

However, legal approaches to image rights differ significantly in terminology, doctrinal grounding, and enforcement mechanisms (Edema & Ecoma, 2024; Mostruat & Cruz, 2023). In conti-

nental Europe, image rights are primarily rooted in personality rights (*droits de la personnalité),* which treat image and likeness as extensions of personhood. In France, the *droit à l'image*, codified in Article 9 of the Code Civil and reinforced by Article 8 of the European Convention on Human Rights, protects individuals against the unauthorized reproduction, dissemination, or commercial use of their image, requiring prior consent that is express, specific, informed, and limited in duration, scope, and purpose. Similarly, in Germany, the *Allgemeines Persönlichkeitsrecht* (General Right of Personality), derived from Articles 1(1) and 2(1) of the *Grundgesetz* (Basic Law), anchors image protection in human dignity and personal autonomy while recognizing both moral and economic interests (Mostruat & Cruz, 2023; Westkamp, 2024).

By contrast, the United Kingdom does not recognize a standalone statutory image right, relying instead on overlapping doctrines such as passing off, breach of confidence, misuse of private information, and data protection (Blackshaw, 2019; Oke, 2024). The United States adopts a more explicitly commercial approach. Originating in privacy jurisprudence, rooted in Warren and Brandeis's (1890) seminal concept of the '*right to be let alone*'. Prosser (1960) classified privacy torts as including the appropriation of name or likeness, laying the groundwork for the right of publicity. Landmark cases such as *Haelan Laboratories Inc. v. Topps Chewing Gum Inc.* (1953) recognized a transferable commercial interest in personal likeness, later affirmed in *Zacchini v. Scripps-Howard Broadcasting Co.* (1977). Under this model, personal likeness is treated as a transferable and licensable economic asset capable of commercial exploitation (McCarthy & Schechter, 2023; Mostruat & Cruz, 2023).

This dual nature of image rights is reflected in the Nigerian case of *Banire v. NTA-Star TV Network Limited* (2021), where the Court of Appeal defined image rights as encompassing publicity rights to wit 'a person's right against misappropriation of his name, likeness, physical appearances, nicknames, pictures,

personal slogans etc., i.e. the right to control the public's commercial exploitation of one's identity'.

Image rights therefore possess a dual legal character, combining privacy-based and property-based interests (Mostruat & Cruz, 2023). The privacy-based model, predominant in continental Europe, emphasizes human dignity, moral integrity, and personal autonomy. Under this approach, likeness is treated as an inalienable extension of personhood, with legal protection arising from the intrinsic relationship between the individual and their persona (Logeais & Schroeder, 1998). Conversely, the property-based model, predominant in the United States, treats likeness as a marketable commodity capable of licensing and economic exploitation (McCarthy & Schechter, 2023). Here, persona becomes a commercial resource, especially in relation to celebrities and public figures, reflecting liberal individualism and market-based understandings of identity (McCarthy & Schechter, 2023). Thus, while the European model emphasizes the inseparability of image and self, the American model reflects liberal individualism, framing likeness as a tradable commodity.

These doctrinal distinctions reveal the predominantly individualistic assumptions underpinning contemporary image rights frameworks. While European jurisdictions have traditionally emphasized dignity, privacy, and personality, and the United States has placed greater emphasis on the commercial exploitation of identity, neither model is exclusively dignitarian or commercial (Logeais & Schroeder, 1998; Mostruat & Cruz, 2023). Rather, both recognize personal and economic interests in differing proportions (Logeais & Schroeder, 1998; Mostruat & Cruz, 2023). The shared premise, however, is that likeness is fundamentally an attribute of the individual rights-holder. This individual-centered conception leaves little conceptual space for forms of likeness that derive their meaning from collective identity, cultural authority, or communal custodianship.

B. African Philosophies: Relational Identity and Communal Cultural Imagery

While Western legal traditions often conceptualize likeness through individualistic and proprietary frameworks, African philosophical traditions situate personhood within networks of social, moral, and communal relationships. The individual is not conceived as an isolated autonomous entity but as a being whose identity is constituted through participation in communal life (Gbadegesin, 1991; Ikuenobe, 2018a, 2018b). African traditional societies are frequently characterized as communitarian, emphasizing that to be human is to belong, to participate, and to nurture social bonds (Mbiti, 1970; Menkiti, 1984; Gyekye, 1997). This communitarian orientation has profoundly influenced African philosophical thought and continues to inform legal and constitutional discourse across many African jurisdictions.

This characterization, however, should not be understood as suggesting that African societies are culturally homogenous or uniformly communitarian. African communitarianism is itself the subject of extensive scholarly debate, with philosophers differing on the nature and extent of communal obligations, the place of individual autonomy, and the relationship between community and rights (Gyekye, 1997; Matolino & Kwindingwi, 2013; Metz, 2018). Scholars have cautioned against essentializing Africa as culturally homogeneous or portraying communal values as inherently incompatible with individual autonomy (Gyekye, 1997; Ikuenobe, 2006, 2018a). African societies have long accommodated varying degrees of individual autonomy within broader communal frameworks, while differences in culture, religion, history and legal traditions have produced diverse understandings of personhood and social organization (Gyekye, 1997; Ikuenobe, 2006; Kahaka & Maundeni, 2022). Moreover, African societies are socially, culturally, and politically diverse, and their conceptions of identity have evolved through urbanization, constitutional development, migration, technological change, and globalization (Gyekye, 1997; Mamdani, 1996). Consequently, communitarian

values should be understood not as a fixed empirical description of all African societies but as a normative philosophical tradition that continues to shape understandings of personhood, dignity, and social responsibility while coexisting with individual rights and liberal constitutional values.

Within this normative tradition, personhood is therefore generally understood as relational rather than exclusively individualistic. This worldview is reflected in aphorisms such as the Southern African maxim *umuntu ngumuntu ngabantu* ('a person is a person through other persons') and John Mbiti's (1970) well-known observation that 'I am because we are, and since we are, therefore I am' (p. 141). These expressions articulate the philosophical foundations of Ubuntu and related communitarian traditions, emphasizing that individual dignity and social recognition are realized through relationships, participation, reciprocity, and communal belonging.

African philosophers including Menkiti (1984), Senghor (1964), Gyekye (1997), Nyerere (1968) and Kenyatta (1965) similarly affirm the centrality of community in the formation of identity. Menkiti (1984) argues that personhood is achieved through moral participation in communal life rather than automatically conferred at birth, while Senghor (1964) observes that 'Negro-African society puts more stress on the group than on the individual, more on solidarity than autonomy' (p. 49). Kenyatta (1965) highlights that individual identity is secondary to social embeddedness: 'nobody is an isolated individual; first and foremost, he is several people's relative and several people's contemporary' (p. 297). Julius Nyerere's *Ujamaa* philosophy also underscores the interdependence of individual welfare and communal well-being (Nyerere, 1968, p. 39). Gyekye (1996) advances a more moderate conception of communitarianism in which communal belonging and individual autonomy are complementary rather than mutually exclusive (pp. 105–106).

Kahaka & Maundeni (2022) also reject a rigid dichotomy between communitarianism and individualism, arguing in-

stead that individuals move between communal and autonomous modes depending on the social setting in which identity is expressed (Nnaemeka, 2023). Their analysis has important implications for the legal framework proposed in this article. It suggests that neither exclusively individualistic nor exclusively communal approaches adequately capture the complexity of identity in contemporary African societies (Kahaka & Maundeni, 2022; Nnaemeka, 2023). Instead, the governance of AI-generated imagery should depend on the nature of the image and the interests it embodies. Images that primarily represent individual identity may appropriately remain subject to personality and privacy rights, whereas images depicting communal rituals, traditional attire, sacred symbols or other culturally significant representations engage collective cultural interests that justify community participation, collective authorization and culturally specific governance mechanisms. Kahaka and Maundeni's (2022) relational conception of personhood therefore provides a theoretical foundation for the concept of communal cultural-image governance, enabling individual dignity and collective cultural responsibility to coexist rather than operate as competing legal values.

Together, these philosophical traditions have important implications for understanding communal cultural imagery. In many African societies, visual identity frequently carries collective, spiritual, and ancestral significance beyond individual representation. Scarification patterns, ceremonial attire, hairstyles, ritual gestures, masquerades, indigenous symbols, and traditional artistic motifs often function as visual markers of communal belonging, lineage, spirituality, and cultural continuity (Drewal, 1992; Takim & Ozim, 2025). Their meaning is therefore not exhausted by individual ownership or commercial value.

Among the Yoruba, for example, ancestral masquerades (*Egungun*) and ritual performances are governed by lineage structures and cultural protocols that regulate their reproduction and public display (Drewal, 1992; Takim & Ozim, 2025). The

Maasai similarly assert collective interests in the commercial use of Maasai names, attire, aesthetics, and cultural representations (Brindle & Florman, 2021; Maasai Intellectual Property Initiative, n.d.). San communities of Southern Africa regard rock art and cultural imagery as shared heritage embedded within communal memory and spiritual meaning (Blundell, 1998; Coronel & Coronel, n.d.). In these contexts, unauthorized reproduction or commodification of this cultural heritage constitutes not merely economic exploitation but also cultural harm, spiritual violation, and communal disrespect (Janke, 1995, 1998, 2003; United Nations General Assembly [UNGA], 2007, Articles 11, 12, 15 and 31).

Another example is provided by the experiences of the San communities, who historically encountered significant disrespect in engagements involving photography, research, and cultural documentation. Researchers reportedly photographed individuals in their homes, breastfeeding mothers, and underage children, without regard for San social norms or customary protocols, while community leaders were bypassed and promises of feedback or reciprocity frequently ignored (San Code of Ethics, 2017). In such contexts, these actions translated into harms to relational identity and communal belonging.

These experiences reflect a broader African philosophical understanding that identity and representation are embedded within social relationships and communal recognition rather than confined to isolated individual autonomy. *Ubuntu*, a core concept in Southern African philosophy, therefore, provides an important normative framework for understanding why harm to representation may also constitute harm to communal dignity and social cohesion. It represents the moral foundation of human coexistence, calling for kindness, compassion, hospitality, and solidarity. As Desmond Tutu (1999) explains:

> 'We say a person is a person through other people. It is not 'I think therefore I am.' It says rather: 'I am human because I belong. I participate, I share. Harmony, friendliness, community are great goods. Social harmony is for

> us the summum bonum — the greatest good. Anything that subverts or undermines this sought-after good is to be avoided like the plague.' (p. 35)

Thus, *Ubuntu* enshrines humanness as an interdependent state, rejecting atomistic individualism, and emphasizing that every action and inaction must serve both self and community (Matolino & Kwindingwi, 2013; Menkiti, 1984, pp. 171-172). Thus, identity is not merely personal but socially constituted and morally embedded (Metz, 2011; Tutu, 1999). Under this framework, representations of culturally significant imagery implicate broader ethical obligations extending beyond individual consent or commercial licensing (Brindle, & Florman, 2021; SAN Code of Ethics, 2017). Communities therefore possess legitimate interests in determining how culturally significant representations are reproduced, circulated, or commercialized. As such, these perspectives suggest that certain forms of identity, including culturally significant images and likenesses, may embody both individual and collective interests. It is this relational understanding of identity that informs the analysis developed in this article.

Consequently, communal cultural rights, concern collectively held interests in traditional cultural expressions, sacred symbols, ritual practices, indigenous aesthetics, and other manifestations of communal heritage and identity. These rights are not centered on individual ownership or commercial personality, but rather on collective custodianship, cultural continuity, spiritual significance, and communal dignity. They are commonly governed through customary law, cultural heritage frameworks, folklore protections, and emerging principles relating to indigenous knowledge and traditional cultural expression governance (UNGA, 2007; WIPO, 2012). Such imagery may include sacred symbols, traditional attire, scarification patterns, ritual gestures, indigenous artistic motifs, hairstyles, ceremonial expressions, and other traditional cultural expressions governed through customary norms and communal custodianship rather than individual ownership.

This relational understanding of identity challenges Western legal frameworks that conceptualize likeness exclusively through individual property or privacy rights. Existing intellectual property and image rights doctrines frequently fail to account for the collective and spiritual dimensions of identity embedded within communal cultural imagery. At the same time, conventional cultural heritage frameworks often inadequately protect living and evolving forms of visual identity (Janke, 1998; Oguamanam, 2020; Ndubisi, 2024). These limitations become particularly acute in the context of AI systems capable of extracting, reproducing, and generating culturally significant representations on a scale.

C. From Relational Identity to Digital Futures

AI is transforming the creation, reproduction, and circulation of likeness and cultural imagery. Generative AI systems capable of autonomously producing images, audio, video, and text are increasingly trained on massive datasets scraped from the internet, museum archives, social media platforms, ethnographic collections, and digital repositories (Guadamuz, 2024; WIPO, 2024a). These datasets frequently include copyrighted works, photographs, biometric information, indigenous cultural materials, and culturally sensitive imagery collected without meaningful consent, attribution, or compensation (Hayes, 2023; Ndubisi, 2024).

From a technical standpoint, generative models develop probabilistic associations between textual prompts and visual forms by analyzing patterns across millions or billions of image-text pairs (Goodfellow et al., 2016). This learning process mirrors early human learning; repeated encounters with labeled objects lead to the formation of conceptual categories, though at a scale and opacity that complicates legal traceability and accountability (McMullan & Stasiuk, 2025). Once trained, an AI model develops a statistical expectation of what objects, persons, or cultural motifs 'look like', synthesizing patterns from its train-

ing data rather than directly copying any specific work (Guadamuz, 2026). These expectations are not neutral. They reflect the cultural, racial, and geopolitical biases embedded in the datasets themselves (Birhane, 2020, p. 404).

Diffusion-based systems such as Stable Diffusion and DALL-E generate outputs by transforming random noise into coherent images based on learned statistical patterns (Rombach et al., 2022; WIPO, 2024a). A prompt such as *'a Maasai elder in traditional attire',* may therefore produce a visually persuasive image that is novel despite no direct relationship existing between the generated representation and the communities whose imagery informed the model's training data (Karras et al., 2021; Radford et al., 2021). Thus, while generative AI outputs may appear novel or transformative, they nevertheless raise questions concerning derivative use, moral rights, and compliance with cultural protocols governing communal heritage.

Importantly, however, not all AI-generated outputs necessarily constitute copyright infringement or unlawful appropriation of culturally sensitive images (Guadamuz, 2026). Because generative AI systems typically generate content through probabilistic pattern synthesis rather than direct copying, many outputs may not reproduce any single protected work or cultural expression with sufficient similarity to satisfy conventional infringement thresholds (Sag, 2024; Guadamuz, 2024; 2026). This has generated significant debate within contemporary scholarship and litigation. Some scholars argue that certain AI-generated outputs may be sufficiently 'transformative' or non-expressive to fall outside traditional copyright liability, particularly where no identifiable source material can be traced in the final output (Sag, 2024). Similarly, ongoing disputes such as *Getty Images v Stability AI* and *Andersen v Stability AI, Midjourney & DeviantArt* illustrate continuing uncertainty regarding whether generative AI constitutes unlawful reproduction, derivative use, or merely statistical learning from underlying datasets (George Washington University Law School, 2025; Guadamuz, 2024; 2026).

Nevertheless, the absence of direct copyright infringement does not eliminate broader ethical, dignitary, or cultural concerns. AI-generated representations may still reproduce culturally recognizable aesthetics, ceremonial attire, indigenous symbols, hairstyles, or ritual imagery in ways that distort cultural meaning, reinforce stereotypes, or violate communal cultural protocols, even where no protected work has been copied verbatim (Fitch et al., 2023; Ndubisi, 2024). In such cases, the harm arises less from conventional infringement than from decontextualization, cultural distortion, or unauthorized extraction of communal identity.

Moral-rights concerns may also arise where AI-generated outputs alter or derogatorily reproduce culturally significant representations associated with identifiable communities or creators. Scholars increasingly argue that existing copyright frameworks inadequately address these relational and communal dimensions of cultural harm (Janke, 2025a; Oguamanam, 2020). Consequently, the central issue is not simply whether AI outputs infringe existing intellectual-property rights, but whether current legal frameworks can address the broader cultural, ethical, and relational harms arising from AI-mediated reproduction of culturally significant imagery.

These developments raise significant concerns regarding both individual image rights and communal cultural rights. At the individual level, generative AI facilitates the creation of deepfakes, synthetic avatars, and biometric simulations capable of reproducing identifiable persons without consent. Such uses may infringe privacy, dignity, publicity, and personality interests while enabling disinformation, reputational harm, identity theft, and commercial exploitation. At the communal level, AI systems also reproduce and commodify communal cultural imagery detached from its social, spiritual, and historical contexts. Because generative models reproduce the biases, omissions, and distortions embedded in their training data, they frequently misrepresent culturally specific identities (Birhane, 2020; Salami, 2024).

Reports from the National Indigenous Times (cited in McMullan & Stasiuk, 2025), document instances where Adobe's stock platform hosted AI-generated images labeled as depicting 'Indigenous Australian' even though these outputs bore little resemblance to Aboriginal or Torres Strait Islander peoples. Several images incorporated arbitrary or fabricated body markings that lacked cultural meaning, effectively trivializing designs that hold ceremonial or spiritual significance (McMullan & Stasiuk, 2025). The same reporting raised concerns about the availability of 'AI-generated Aboriginal artwork' for commercial use, prompting fears that genuine Indigenous artworks had been ingested into training datasets without artists' knowledge or consent (McMullan & Stasiuk, 2025).

Early Midjourney outputs labeled 'Indigenous Australians', which in fact resembled African ethnic groups demonstrate how generative AI systems can flatten culturally distinct identities into generic or distorted racialized aesthetics (McMullan & Stasiuk, 2025). Although this example arises from the Australian context, it is included as a comparative illustration of broader Indigenous concerns regarding AI-generated cultural imagery, particularly the risk of cultural homogenization, misrepresentation and unauthorized appropriation. These concerns resonate across many Indigenous and traditional communities globally, including in Africa, where AI systems may similarly generate synthetic tribal imagery, sacred symbols, traditional hairstyles, artistic styles, or ritual aesthetics without community authorization, cultural understanding or respect for customary governance (Kasosi, 2025).

These practices contribute to what Dugeri (2024) refers to as 'rights laundering', whereby copyrighted or culturally significant materials are reproduced by AI systems stripped of attribution, authorship, or cultural meaning (Birhane, 2020; Ndubisi, 2024). The scale of this challenge is underscored by a 2024 admission by an OpenAI representative before the UK Parliament that 'it would be impossible to train today's leading AI models without

using copyrighted materials' (Al-Sibai, 2024; OpenAI, 2023). This admission suggests that generative AI, as presently constituted, relies extensively on unlicensed materials, including works protected by moral rights, and potentially, culturally sensitive images, materials subject to collective custodianship, and cultural protocols.

Scholars increasingly characterize these dynamics as forms of data or algorithmic colonialism (Birhane, 2020; Couldry & Mejias, 2019; McMullan & Stasiuk, 2025; Ndubisi, 2024; Salami, 2024). Under this framework, human identity and cultural life are transformed into extractable data resources for technological industries, frequently without governance, reciprocity, or benefit-sharing (Birhane, 2020; McMullan & Stasiuk, 2025). Generative AI, therefore, extends historical patterns of colonial extraction into digital environments, reproducing asymmetries of power within global knowledge and image economies (Birhane, 2020).

The opacity of AI development compounds these challenges. Training datasets are rarely disclosed, licensing arrangements are inconsistent, and legal liability for infringement is diffused across developers, deployers, and data intermediaries (Guadamuz, 2024). For Indigenous communities, this opacity has significant implications. Although communal cultural expressions are often treated as de facto public domain once digitized, they are not free from legal, moral, or cultural constraints (Okediji, 2018). As Guadamuz (2024) note, digital reproductions may attract their own layer of copyright protection, meaning that incorporating them into AI training datasets can constitute infringement. In jurisdictions such as the United States, the fair use doctrine currently allows the ingestion of copyrighted material for the purpose of training foundation models (Weslow et al., 2025). However, this exception is not absolute. If an AI system generates outputs that are substantially similar to copyrighted works, especially where such outputs act as a substitute for, or otherwise affect the commercial market of, the original, then the fair use shield may no longer apply to the resulting output (Getty

Images v. Stability AI; Guadamuz, 2026; Weslow et al., 2025). In such cases, the protections that apply at the training stage may not extend to the model's generative behavior, exposing developers or users to potential liability (Guadamuz, 2024). More importantly, such incorporation violates principles of Indigenous Data Sovereignty, which assert the right of Indigenous peoples to control the collection, access, and use of data about their cultures and communities (Ndubisi, 2024; Oguamanam, 2019).

D. Communal Cultural Imagery and Traditional Cultural Expressions

Across many African societies, images, symbols, attire, performances, and visual expressions frequently embody broader communal, spiritual, and cultural meanings tied to ancestry, social belonging, and collective dignity (Ndubisi, 2024). This relational understanding of likeness reflects African philosophical traditions in which personhood is constituted through relationships, communal recognition, and moral interdependence rather than through isolated individual autonomy (Mbiti, 1970; Menkiti, 1984; Ramose, 1999).

Likewise, in many African societies, a person is understood not merely as an isolated individual but as deeply connected to the honor, dignity, and reputation of the family or community (Akpa-Inyang & Chima, 2021; Ndubisi, 2024). In Southern African thought, the Nguni expression *umuntu ngumuntu ngabantu* ('a person is a person through other persons') captures this relational understanding of identity associated with Ubuntu philosophy (Mbiti, 1970; Tutu, 1999; Ramose, 1999). Within this framework, harm to an individual's likeness may also produce broader social and communal harm because identity is understood as embedded within relationships, communal recognition, and collective belonging (Ndubisi, 2024). Consequently, culturally significant representations often embody lineage, spirituality, communal authority, and collective memory rather than purely individual identity.

These relational conceptions of identity are particularly evident in relation to communal cultural imagery and traditional cultural expressions. Ritual performances, ceremonial attire, scarification patterns, sacred symbols, indigenous hairstyles, masquerades, dances, and artistic motifs frequently operate not merely as aesthetic objects but as repositories of social meaning, spiritual significance, and cultural continuity (Ndubisi, 2024). Among the Yoruba, for instance, *Egungun* masquerades embody ancestral presence and communal authority, while among the Maasai, attire, jewelry, and visual symbolism communicate age, gender, social status, and communal belonging (Aremu, Banjo, & Olanipekun, 2012; Kasosi, 2025). Such representations therefore implicate broader communal cultural interests extending beyond the autonomy or commercial interests of any individual depicted.

This distinction is important for the purposes of this paper. Unlike individual image rights, which primarily protect the interests of identifiable individuals against the unauthorized use of their likeness, rights in communal cultural imagery concern collectively held interests in culturally significant images linked to heritage, spirituality, identity, and traditional cultural expression. While these categories may overlap, they remain distinct. The harm arising from misuse of communal cultural imagery frequently concerns cultural distortion, communal disrespect, spiritual violation, and loss of cultural integrity rather than solely personal reputational or economic injury (Janke, 1995; La Salle & Commodifications of Cultural Heritage Working Group, 2014).

These relational understandings of identity are increasingly reflected within African legal frameworks governing traditional cultural expressions. Kenya's Protection of Traditional Knowledge and Cultural Expressions Act 2016 provides one of the continent's most developed statutory frameworks for protecting traditional cultural expressions. The Act prohibits the unauthorized commercial exploitation, distortion, or derogatory treatment of protected cultural expressions and requires prior informed consent, equitable benefit-sharing, and respect for cultural proto-

cols (sections 18, 21, and 24). These protections are relevant in relation to Maasai cultural imagery, which has historically been appropriated by global corporations and fashion brands without community consent or compensation. Similarly, Nigeria recognizes collective cultural ownership, particularly through the Copyright Act's (2022) protection of Traditional Cultural Expressions. The Act protects expressions of folklore against unauthorized reproduction, adaptation, or commercial exploitation outside customary contexts (section 74). These provisions recognize that certain cultural expressions belong collectively to communities rather than to individual authors and bearers (section 74(5)). However, enforcement authority remains largely vested in state institutions, limiting direct community control over representations central to communal identity (section 75). South Africa has proposed comparable legislation through the Indigenous Knowledge Bill and related legislative proposals (Protection, Promotion, Development and Management of Indigenous Knowledge Act 6 of 2019). The Bill similarly recognizes communities as custodians of cultural expressions, visual motifs, traditional attire, and indigenous symbols. Although the Indigenous Bill has not yet become fully operational, it is included because it illustrates the direction of legislative reform and reflects increasing recognition that identity and representation may constitute collective cultural interests grounded in continuity, custodianship, and communal dignity.

Collectively, these developments signal growing recognition that culturally significant imagery may embody communal identity, dignity, and heritage in ways not fully accommodated by conventional personality rights, privacy, or copyright frameworks. Although these provisions were not designed specifically to regulate cultural imagery or AI-generated representations, they provide an interpretive foundation through which rights in communal cultural imagery may increasingly be recognized and protected.

E. Contemporary Relevance of Communal Cultural Imagery and Legal Foundations

The challenges posed by generative AI demonstrate the urgent need for legal frameworks capable of recognizing both individual and communal dimensions of likeness. Existing intellectual property, privacy, and publicity doctrines remain insufficient for addressing the cultural, spiritual, and relational harms arising from generative AI. At the same time, traditional cultural heritage protections often inadequately address living representations, performative identities, and digitally reproduced likenesses.

African legal and philosophical traditions nevertheless provide important normative resources for rethinking these issues. Applying Ubuntu to AI ethics suggests that digital likenesses should not be treated purely as individual property but as relational assets embedded within communal moral frameworks (Ndubisi, 2024). African jurisprudence already provides support for this approach. South African constitutional jurisprudence, for example, has consistently invoked Ubuntu to emphasize relational identity, dignity, and social interdependence (Himonga, Taylor, & Pope, 2013; Mokgoro, 1998). In *S v Makwanyane* (1995), the Constitutional Court recognized Ubuntu as embodying humanness, social justice, and fairness. Similarly, in *Port Elizabeth Municipality v Various Occupiers* (2005), the Court observed that:

> 'The spirit of ubuntu, part of the deep cultural heritage of the majority of the population, suffuses the whole constitutional order. It combines individual rights with a communitarian philosophy. It is a unifying motif of the Bill of Rights, which is nothing if not a structured, institutionalized, and operational declaration of the need for human interdependence, respect, and concern'. (*Port Elizabeth Municipality v Various Occupiers*, 2005, para. 37).

While these cases do not address either individual image rights or communal cultural rights specifically, they demonstrate that Ubuntu has been recognized as a constitutional value. This

recognition provides a foundation for arguing that Ubuntu could inform image-rights doctrine, though this application has not yet been judicially tested.

Regional and international instruments similarly recognize collective cultural interests. The African Charter on Human and Peoples' Rights (1981) affirms both individual and peoples' rights, while the Swakopmund Protocol on the Protection of Traditional Knowledge and Expressions of Folklore (2010) recognizes communal interests in cultural expressions. WIPO's ongoing work on Traditional Cultural Expressions further reflects growing international recognition of collective cultural rights (WIPO, 2001; WIPO, 2012).

However, these frameworks remain underdeveloped in relation to AI-generated likenesses and communal cultural imagery. Existing protections primarily address intangible cultural assets rather than digitally generated representations of living identity and communal aesthetics (Chen & Friedmann, 2025). Embedding African philosophies such as Ubuntu into emerging AI governance frameworks therefore offers a basis for developing more context-sensitive and ethically responsive approaches to image rights and communal cultural rights protection.

III. LEGAL FRAMEWORKS FOR IMAGE RIGHTS AND RIGHTS IN COMMUNAL CULTURAL IMAGERY IN AFRICA

The cultural, ethical, and technological challenges posed by generative AI resonate across several African legal systems. In South Africa, Kenya, and Nigeria, histories of colonial dispossession and racialized representation have shaped legal and cultural understandings of dignity, identity, and community. These jurisdictions were selected because they represent influential African legal and digital economies with evolving yet distinct constitutional, statutory, and common-law approaches to privacy, dignity, data protection, personality rights, cultural heritage, and digital governance. While all three jurisdictions are actively

developing legal responses to individual image rights and emerging technologies, they differ in doctrinal emphasis, regulatory development, and judicial articulation. South Africa possesses the most developed dignity-based personality-rights jurisprudence grounded in constitutionalism and Ubuntu philosophy. Kenya has developed an increasingly rights-oriented constitutional and data-protection framework with strong judicial recognition of individual image rights; while Nigeria presents a rapidly evolving hybrid common-law and statutory landscape shaped by constitutional privacy guarantees, intellectual property frameworks, and emerging data-governance reforms. Together, these jurisdictions provide a meaningful spectrum of African legal responses to questions of identity, likeness, communal imagery, and technological harm.

A. Image Rights as Constitutional Dignity and Privacy Interests

Across South Africa, Kenya, and Nigeria, legal protection for interests associated with individual image rights has increasingly developed through constitutional guarantees relating to dignity, privacy, autonomy, and identity. Although the extent of judicial recognition varies considerably across these jurisdictions, the courts in these jurisdictions increasingly recognize that the unauthorized use of a person's likeness implicates fundamental questions of personality, selfhood, and human dignity. South African and, increasingly, Kenyan courts have recognized that the unauthorized use of a person's likeness may implicate constitutional values of dignity, privacy and personality, thereby extending protection beyond traditional intellectual property doctrines. In Nigeria, however, judicial recognition remains more fragmented. Rather than recognizing an autonomous constitutional individual image right, Nigerian law protects aspects of personality through a combination of constitutional rights, intellectual property law, passing off, tort and, more recently, data protection legislation.

In South Africa, protection derives primarily from the common-law *actio iniuriarum* and constitutional guarantees of dignity and privacy under sections 10 (dignity) and 14 (privacy) of their Constitution (Mangope & Alberts, 2022). South African personality rights encompass *corpus* (physical integrity), *fama* (reputation), and *dignitas* (dignity) with courts interpreting *dignitas* broadly to include personal identity, honor, privacy, and control over one's image (Cornelius, 2008; Mangope & Alberts, 2022). The *actio iniuriarum*, rooted in Roman-Dutch law, provides a remedy for willful infringements of these personality interests, allowing both damages and interdicts for violations (Cornelius, 2008; Mangope & Alberts, 2022). Consequently, the unauthorized commercial use of a person's photograph or likeness is treated primarily as an affront to dignity and personality rather than purely as a proprietary harm (Cornelius, 2008; IOL, 2024).

This constitutional grounding is evident in landmark decisions such *as O'Keeffe v Argus Printing & Publishing Co Ltd* (1954), where the court recognized that publishing a person's image for advertising purposes without consent infringes personality rights. This decision set a precedent, affirming that an individual's image and identity are protected interests under South African law. Importantly, the ruling affirmed that commercial exploitation of an individual's likeness requires consent, laying the foundation for modern individual image-rights jurisprudence (Cornelius, 2008, p. 72).

Subsequent decisions refined these principles. In *Grütter v Lombard* (2007), the Supreme Court of Appeal recognized both misrepresentation and commercial appropriation as actionable violations of identity (Cornelius, 2024). Similarly, *Wells v. Atoll Media (Pty) Ltd* (2010) affirmed that even non-celebrities retain enforceable personality rights over the publication of identifiable photographs taken in public spaces, while *Kumalo v Cycle Lab (Pty) Ltd* (2011) confirmed that the unauthorized use of a celebrity's image in advertising infringed dignity, identity, and privacy.

In *Wells,* a magazine published a photograph of a twelve-year-old girl taken on a public beach without her parent's consent. Although her face was not visible, she was identifiable to those who knew her, and she suffered severe embarrassment and harassment once the image circulated. The Western Cape High Court held that the non-consensual publication, even in a public setting, violated her privacy and dignity. The court recognized that public location does not eliminate privacy expectations, and non-celebrities are fully protected under personality rights. In *Kumalo,* former Miss South Africa, Basetsana Kumalo's image was used in an advertising brochure without permission. The Court held that this unauthorized use for commercial gain violated her identity, dignity, and privacy, confirming that personality rights apply in promotional contexts.

Unlike the United States of America's right of publicity and the United Kingdom's regime, South African law does not require fame as a condition for protection. Any individual's identity can be infringed, with damages measured on patrimonial loss (Cornelius, 2008, p. 74; 2011), although a claimant's public recognition may affect the quantum of damages (Cornelius, 2008, p. 75). Cornelius (2008) argues that the South Africa approach is comparatively advanced because it locates identity protection within human dignity, rather than treating it solely as an economic asset (p. 74).

Kenyan courts have similarly grounded individual image rights in constitutional dignity and privacy protections under the Constitution of Kenya, 2010. The Constitution of Kenya (2010) guarantees the rights to human dignity (Article 28), privacy (Article 31), and property (Article 40), which Kenyan courts have consistently interpreted as extending to control over one's image and likeness (Netsheria, 2021; Ogonjo, 2023).

Although Kenyan courts have progressively recognized image-related interests through constitutional guarantees of dignity, privacy, autonomy and, more recently, data protection, they have not expressly grounded these protections in African philos-

ophies of personhood, Ubuntu or other communitarian conceptions of identity. Rather, the existing jurisprudence has developed within a constitutional rights framework that emphasizes individual dignity, privacy and personal autonomy. This article does not suggest otherwise. Instead, it advances a normative argument that African philosophies of personhood provide a valuable interpretive resource for developing a more coherent framework for regulating image rights, particularly where AI-generated imagery implicates communal cultural identity and collective interests. The reliance on Ubuntu and related communitarian traditions is therefore not presented as a description of current Kenyan jurisprudence but as a normative framework capable of complementing existing constitutional protections by addressing the collective dimensions of culturally significant imagery that individual rights-based approaches do not adequately capture.

Kenyan courts have progressively articulated the contours of an individual image-rights claim. In *Jessicar Clarise Wanjiru v Davinci Aesthetics & Reconstruction Centre* (2017), the High Court expressly recognized image rights as part of Kenyan law, distinguishing between privacy-based protection against non-consensual exploitation and publicity-based control over the commercial value of one's persona. The Court articulated a tripartite test requiring: (i) use of a protected aspect of identity; (ii) an exploitative purpose; and (iii) absence of consent.

Subsequent decisions reinforced this constitutional approach. In *Ann Njoki Kumena v KTDA Ltd* (2019), the unauthorized use of a worker's photograph in marketing materials was held to violate constitutional rights to dignity, privacy, and property. Similarly, in *Catherine Njeri Wanjiru v Machakos University* (2021), where a university used a student's graduation photograph in promotional materials without permission, the High Court at Machakos recognized that a person's image constitutes a core aspect of personality and autonomy, affirming that individuals possess the right to control publication and commercial use of their likeness. The Court awarded damages and ordered

removal of the image, emphasizing both the dignitary and economic dimensions of individual image rights.

Kenyan courts have increasingly linked individual image rights to the constitutional right to property, particularly for unauthorized commercial use. This approach is evident in *Machakos University* (2021) and in *Kuria v University of Kabianga* (2023), where a student successfully challenged the use of his image in institutional advertising. In both cases, courts emphasized that commercial exploitation of an image without consent amounts to an unlawful appropriation of something of value belonging to the individual, warranting compensatory relief.

Notably, in *Mutuku Ndambuki Matingi v Rafiki Microfinance Bank Limited* (2021), the Kenyan High Court drew persuasive guidance from South African authorities such as *Grütter v Lombard* and *Wells v Atoll Media*, in addressing the unauthorized commercial use of the petitioner's photograph in a loan advertisement (Cornelius, 2024). The Court held that the unauthorized use of a person's likeness for commercial purposes violated the constitutional right to human dignity under Article 28 of the Kenyan Constitution. In doing so, the Court relied on South African personality-rights jurisprudence to reinforce the protection of individual image rights within Kenya's constitutional framework (Cornelius, 2024).

Nigerian courts have likewise begun recognizing individual image rights through constitutional privacy and dignity principles, although the doctrinal development has been inconsistent. Section 37 of the 1999 Constitution guarantees the right to privacy, a provision that Nigerian courts and scholars have interpreted to encompass personal information and elements of identity, including an individual's likeness (Nwabueze & Olumekor, 2021). Although the constitutional text refers primarily to the privacy of the home, correspondence, and communications, judicial interpretation has extended its scope to visual and biometric identifiers. In *Emerging Markets Telecommunication Services v Eneye* (2018), the Supreme Court of Nigeria affirmed that con-

stitutional privacy protects personal data and identity markers such as photographs and biometric information. Similarly, the Court of Appeal of Nigeria in *Nwali v Ebonyi State Independent Electoral Commission* (*EBSIEC)* (2014) held that the unauthorized commercial use of a person's image infringes both privacy and dignity.

Historically, Nigerian courts approached disputes involving the unauthorized use of a person's image primarily through copyright law or passing-off frameworks. This constraint was evident in *Oluwadamilola Banire v NTA-Star TV Network Ltd* (2021), where a television presenter challenged the promotional use of her photographs on billboards without her consent. Both the Federal High Court and the Court of Appeal dismissed the claim on the basis that copyright vested in her former employer. The courts treated copyright ownership, rather than personal image or dignity, as determinative, effectively excluding claims grounded solely in the misuse of likeness.

However, recent decisions increasingly recognize personality-based claims independent of copyright ownership. This shift is evident in *Ubom v Globacom (Nig) Ltd* (2023/2025). Globacom had used the claimant's photograph on billboards to advertise a reality television singing competition without her consent. Lower courts dismissed the suit on jurisdictional grounds, accepting the argument that the dispute was essentially about copyright and therefore fell within the exclusive jurisdiction of the Federal High Court. The Supreme Court rejected this narrow characterization. It held that the unauthorized commercial use of an individual's image constitutes a distinct violation of personality rights, analytically separate from copyright in the photographic work. The Court emphasized that the gravamen of the claim lay in the unauthorized use of the claimant's likeness to imply endorsement not in authorship or ownership of the photograph.

Similarly, in *Ndidi-Amaka Odogwu v Quilox Restaurant & Bar Ltd* (2017), the plaintiff, a former beauty pageant contestant, challenged the unauthorized use of her photograph in

promotional materials for a nightclub event circulated on social media platforms. The defendant argued that the image was sourced online and that its public availability implied consent. The Federal High Court rejected this contention, holding that online availability does not extinguish the requirement of consent. It found that the commercial use of the plaintiff's image violated her constitutional rights to dignity and privacy under sections 34(1) and 37 of the 1999 Constitution, particularly given the false association created and the impact on her personal and religious identity. The decision affirmed that individuals retain enforceable control over the commercial use of their likeness irrespective of where the image is sourced. The judgment thus solidifies the constitutional basis of individual image rights and signals that both public figures and private individuals may seek relief for non-consensual use of their likeness (Abdulsalam, et al., 2025).

More recently, in *Adunni Adewale v Polanc Media Ltd* (2025), the respondents published the applicant's name and photograph in an online story entitled *'Six Popular Nigerian Celebrities Who Have Been Accused of Dating Dino Melaye'*. A Lagos High Court held that publishing the applicant's photograph and name in an online article falsely linking her to alleged misconduct violated her rights to dignity and privacy under the Constitution, as well as her data-protection rights under the Nigeria Data Protection Act 2023. The Court rejected claims of implied consent arising from the applicant's public social-media presence, emphasizing that widespread availability of personal images does not negate constitutional protections. It awarded damages and ordered deletion of the offending content, reaffirming that individuals retain ongoing control over the use of their likeness in digital environments.

Consequently, while Nigerian law does not formally recognize individual image rights, judicial reasoning reflects an implicit acknowledgement that individuals, whether celebrities or private persons, have a legitimate interest in controlling the use

of their likeness (Nwabueze & Olumekor, 2021; Olubiyi et al., 2020).

Together, these jurisdictions reveal an emerging trend that individual image rights are fundamentally connected to dignity, identity, and autonomy rather than merely to commercial exploitation. South African jurisprudence remains the most doctrinally developed, particularly through its dignity-centered personality-rights framework, while Kenyan courts have increasingly constitutionalized image protection through rights-based reasoning. Nigeria's approach, remains comparatively underdeveloped and doctrinally fragmented, underscoring the need for a more coherent framework. However, Nigerian courts are progressively moving beyond narrow copyright analysis toward recognition of personality-based image rights grounded in privacy and dignity. The decisions in *Adunni* and *Quilox* are particularly significant because they suggest that the public availability or online sourcing of photographs does not extinguish the underlying dignity and privacy interests attached to an individual's likeness, thereby implying that AI developers and dataset curators should remain subject to obligations of consent, dignity, and privacy even where images used for AI training are scraped from publicly accessible digital platforms.

B. Individual Image Rights Through Data Protection and Digital Privacy Frameworks

Data protection law has become an increasingly important mechanism for regulating individual image rights in the digital age. In South Africa, Kenya, and Nigeria, photographs, facial images, biometric identifiers, and other visual representations are increasingly recognized as forms of personal data subject to consent-based processing requirements. These developments are particularly significant in the context of AI systems that rely heavily on facial recognition technologies, biometric extraction, and the large-scale processing of visual data.

South Africa's Protection of Personal Information Act 4 of 2013 (POPIA) classifies photographs, facial images, and biometric identifiers as 'personal information' requiring lawful processing grounded in consent, purpose specification, and minimality (section 11). Section 71 further restricts certain forms of automated decision-making, while section 24 provides individuals with a qualified right to request deletion of personal information, which can be seen as a limited form of the 'right to be forgotten' (Ayalew, 2024). Although POPIA was not drafted specifically for generative AI, its provisions increasingly provide a basis for challenging the unauthorized processing of facial images and biometric likenesses.

Similarly, Kenya's Data Protection Act 2019 classifies identifiable images and photographs as personal data requiring a lawful basis for processing while granting data subjects rights of access, correction, and deletion (sections 25-26). Kenyan courts have increasingly integrated data-protection principles into individual image-rights litigation, treating breaches of data-controller obligations as an additional basis for liability (Ogonjo, 2023). In *Machakos University* (2021), the High Court held that the university acted as a data controller when it processed and published the claimant's graduation photograph without consent, thereby violating both constitutional rights and statutory data-protection obligations. Kenya's Office of the Data Protection Commissioner (ODPC) has also adopted an increasingly interventionist approach to biometric governance, exemplified by the 2023 suspension of the Worldcoin biometric identification project, an AI-driven, biometric identification system based on iris scanning, due to concerns surrounding consent, proportionality, and data protection (Tsebee & Oloyede, 2024).

Nigeria's Data Protection Act 2023 (NDPA) similarly classifies photographs, facial images, and biometric identifiers as personal data (section 65), requiring lawful processing based on consent or other recognized justifications (sections 24-25). The NDPA grants individuals rights to withdraw consent, object to

processing, request deletion, and challenge certain forms of automated processing (sections 34-38). Scholarly commentary and regulatory developments under Nigeria's data protection regime, further reinforce the understanding that likeness forms part of constitutionally protected personal information (Babalola, 2022; Nwabueze & Olumekor, 2021). On this basis, individuals are entitled to determine whether, and under what conditions, their image may be disclosed or used, rendering unauthorized commercial exploitation of likeness potentially actionable as a privacy violation (Atoyebi, 2024). Consequently, the unauthorized use of photographs or AI-generated likenesses may increasingly be framed as unlawful data processing rather than solely as privacy or intellectual-property violations as illustrated in the decision in *Quilox*.

Despite these developments, all three jurisdictions face significant regulatory gaps in relation to generative AI. Existing data-protection frameworks primarily regulate the processing of personal data rather than the creation of synthetic likenesses generated through probabilistic modeling. Generative AI systems may produce convincing representations of identifiable individuals without directly reproducing existing photographs or biometric records (Guadamuz, 2024); thereby complicating the application of traditional data-protection principles. Moreover, none of the three jurisdictions currently impose comprehensive obligations concerning dataset disclosure, biometric scraping, AI training transparency, or synthetic identity generation.

C. Intellectual Property Law and the Protection of Likeness

Although intellectual property (IP) law does not recognize individual image rights as an autonomous legal right, it provides indirect mechanisms for protecting the commercial value of identity through copyright, trademarks, passing off and unfair competition, particularly where a person's image is exploited for commercial gain, used to imply false endorsement, or incorporated into branding and merchandising activities (Blackshaw,

2019; Mostruat & Cruz, 2023; Oke, 2024; Synodinou, 2014). Nevertheless, copyright and trademark regimes across South Africa, Kenya, and Nigeria remain fundamentally limited in addressing likeness as such because traditional IP frameworks were not designed to protect human likeness or identity as autonomous legal interests (Ogbah, et al, 2026; Ojongo, 2023). Instead, these regimes protect creative works, commercial source identifiers and the goodwill associated with them (Mangope & Alberts, 2022; Ogbah, et al, 2026; Ojongo, 2023). This creates important doctrinal overlaps, but also significant gaps, particularly in the context of generative AI and synthetic likenesses (Guadamuz, 2026, 2024, 2017; Samuelson, 2023). Particularly where such AI systems generate or reproduce communal cultural imagery, because the resulting harm extends beyond the unauthorized use of a creative work or commercial sign to encompass communal cultural rights, collective cultural identity, community authority, cultural integrity and the observance of cultural protocols, interests that conventional IP doctrines are not designed to protect (Nwauche, 2015).

Across all three jurisdictions, copyright law generally vests ownership of photographs in the photographer or employer rather than the subject of the image (Ogbah, et al, 2026). Consequently, this limits the ability of individuals whose likeness appears in the photograph to control the use of their own likeness unless they own or acquire copyright in the underlying image. Consequently, disputes involving image misuse have frequently exposed tensions between copyright ownership and personality interests (Gelias LLP, 2025; Synodinou, 2014).

This limitation has been particularly visible in Nigerian jurisprudence. In *Banire v NTA-Star TV Network Ltd*, the courts treated copyright ownership in the photographs as determinative, effectively excluding claims grounded solely in misuse of likeness. The claimant's image and autonomy interests were subordinated to the copyright interests of the employer that owned the images. This demonstrates one of the major tensions

between individual image rights and copyright law; copyright protects the image as a creative work, whereas image rights seek to protect the person represented in the image.

In response to these limitations, courts in Nigeria and Kenya have increasingly moved toward recognizing personality-based claims independent of copyright ownership. Nigerian decisions such as *Ubom*, *Quilox*, and *Adunni* represent a jurisprudential shift away from purely copyright-centric reasoning toward recognition of likeness as an aspect of dignity, privacy, and personal identity. Similarly, Kenyan courts in *Machakos University*, *Kumena*, and *Wanjiru* recognized that unauthorized commercial use of an image implicates constitutional dignity and autonomy irrespective of who owns copyright in the underlying photograph.

Trademark law also intersects with individual image rights, particularly in relation to commercially valuable identities and celebrity branding. In Nigeria, public figures increasingly register names, slogans, stage names, and catchphrases as trademarks to prevent unauthorized commercial exploitation of persona. Examples include the registration of 'Star Boy' by Wizkid and the name 'OMOTOLA' by Omotola Jalade-Ekeinde (Nwabueze & Olumekor, 2021). Trademark law therefore enables limited control over commercially identifiable aspects of personality where those features function as source identifiers in trade.

Similarly, the tort of passing off operates across Kenya and Nigeria as a mechanism for protecting commercial goodwill associated with a person's likeness or identity (Nwabueze & Olumekor, 2021; Olubiyi, et al., 2020; Ogonjo, 2023). Where the unauthorized use of an image falsely implies endorsement, sponsorship, or affiliation, litigants may bring claims based on misrepresentation and injury to goodwill (Nwabueze & Olumekor, 2021; Olubiyi, et al., 2020). Nigerian celebrity disputes involving comedian Emmanuel Ejekwu ('Sabinus') illustrated how litigants can combine the trademark infringement and passing-off doctrines to challenge the exploitative commercial use of a persona. Sabinus challenged the unauthorized use of animated car-

icatures of his likeness or his registered catchphrase 'Something Hooge' in advertisement campaigns (Mudasiru, 2022; Tariemi, 2022). The trademark disputes were ultimately resolved amicably (Ani, 2026).

South African law intersects with intellectual property somewhat differently because its personality-rights framework is comparatively more developed. Rather than relying primarily on copyright or passing off, South African courts protect likeness through the *actio iniuriarum* and related personality-rights doctrines grounded in dignity, identity, privacy, and reputation (van Gensen, 2023). Cases such as *Grütter*, *Wells*, and *Kumalo* demonstrate judicial recognition that unauthorized commercial use of a person's likeness constitutes an actionable infringement of identity and dignity independent of copyright ownership. At the same time, intellectual property nevertheless intersects with individual image rights in commercial contexts involving advertising, merchandising, endorsement, and branding, where likeness acquires significant economic value. As van Gensen (2023) further notes, South African law increasingly acknowledges the patrimonial harm that may arise from the unauthorized commercial exploitation of an individual's image, particularly within celebrity merchandising and digital media environments.

Despite these developments, traditional IP law remains ill-suited to addressing many contemporary forms of image misuse, particularly those arising from AI-generated likenesses (Guadamuz, 2024; 2026; Westkamp, 2024). Copyright law protects the photograph or artistic work rather than the person depicted (Guadamuz, 2017; Samuelson, 2023); trademark law protects commercial indicators rather than identity (Dogan & Lemley, 2006); and passing off affords protection only where goodwill, misrepresentation and resulting damage can be established, such as in cases of false endorsement (Oke, 2020; Irvine *v Talksport Ltd*, 2002).

D. Limits of Existing Intellectual Property and Individual Image-Rights Frameworks

Despite these developments, existing individual image-rights and IP regimes in South Africa, Nigeria and Kenya continue to afford limited protection for rights in communal cultural imagery and traditional cultural expressions. While regional and national instruments, including the Swakopmund Protocol and Kenya's Protection of Traditional Knowledge and Cultural Expressions Act 2016, recognize collective rights and community authorization, protection remains fragmented and is largely grounded in intellectual-property concepts of authorship, originality, fixation and commercial exploitation as the primary bases of legal protection (Boateng, 2011; Nwauche, 2015; Oguamanam, 2023; WIPO, 2024). Nigeria continues to rely primarily on conventional intellectual property doctrines and limited statutory protection for folklore, illustrating the continuing gap between communal cultural values and inherited legal frameworks (Nigeria Copyright Act, 2022, s. 74).

Indigenous cultural expressions, by contrast, are often collective in origin, custodianship, and meaning, emerging through communal participation, intergenerational transmission, and shared cultural practice rather than through isolated acts of individual creation and fixed work (Janke, 1998, p. 8; Oguamanam, 2006, p. 158).

Legislative developments across these jurisdictions nevertheless reflect growing recognition that conventional copyright frameworks inadequately capture the nature of communal creativity. Section 74 of the Nigerian Copyright Act 2022 protects expressions of folklore against unauthorized reproduction and commercial exploitation; section 21 of Kenya's Protection of Traditional Knowledge and Cultural Expressions Act 2016 recognizes community rights over traditional cultural expressions and requires prior informed consent and equitable benefit-sharing; while section 28D of the South African Copyright Act, which is currently not in operation and awaiting proclamation by the

South African president, acknowledges communal interests in indigenous cultural expressions. Collectively, these provisions signal emerging departures from orthodox Western models by recognizing that certain forms of creativity and representation are communal rather than purely individual in character.

However, traditional cultural expressions are not static artifacts capable of easy categorization within conventional copyright systems. They are dynamic, evolving, and performative, transmitted and renewed through ritual, oral tradition, ceremonial practice, and communal participation. Their meaning frequently derives from spiritual obligations, customary norms, and social relationships that extend beyond economic exploitation or individual ownership (Janke, 1998, pp. 7-8). Consequently, many communal cultural imageries remain poorly suited to legal frameworks designed primarily around fixed works attributable to identifiable individual authors.

As a result, many communal cultural expressions fail to satisfy conventional copyright thresholds relating to originality, fixation, or identifiable authorship and are therefore frequently treated as part of the public domain, despite continuing cultural, spiritual, and communal significance (Lawal-Arowolo, 2015; Oguamanam, 2006, pp. 158, 160; Okediji, 2018). This significantly limits the ability of communities to control how communal cultural imagery is reproduced, contextualized, or commercialized.

Copyright exceptions such as fair use and fair dealing further intensify these vulnerabilities in the context of generative AI. Although originally designed to facilitate socially beneficial activities such as research, education, commentary, and innovation, these doctrines increasingly provide legal justification for large-scale scraping, reproduction, and algorithmic analysis of visual and cultural materials without meaningful consent, attribution, or compensation (Reed, 2019; Sag, 2024). AI developers frequently rely on expansive interpretations of fair use to ingest digitized archives, photographs, artworks, ethnographic mate-

rials, and culturally significant imagery into training datasets used to develop generative systems (Guadamuz, 2026; 2024).

Contemporary disputes, including *Getty Images v Stability AI,* illustrate how AI training practices challenge existing IP frameworks and expose significant governance gaps relating to communal cultural imagery and communal identity (George Washington University Law School, 2025). Although such disputes are typically framed through copyright doctrine (Sag, 2024), they may also reveal broader concerns regarding extractive data practices that disproportionately affect indigenous and marginalized communities whose cultural materials are incorporated into AI systems without consultation or benefit-sharing (Ndubisi, 2024).

African legal instruments have taken important steps toward addressing some of these concerns. Frameworks such as the Swakopmund Protocol (2010), Kenya's Protection of Traditional Knowledge and Cultural Expressions Act 2016, and Nigeria's folklore protections recognize communal interests in traditional knowledge and cultural expressions, require forms of prior informed consent, and incorporate benefit-sharing principles. These frameworks align more closely with the collective and relational nature of indigenous creativity by recognizing that communal cultural imagery may embody communal identity, heritage, spirituality, and collective dignity rather than merely economic value.

Nevertheless, these protections remain limited in important respects. Many operate territorially; depend on formal documentation or registration or focus primarily on traditional cultural expressions rather than digitally reproduced or AI-generated representations. Oral traditions, evolving practices, performative identities, and culturally embedded visual expressions frequently remain outside their effective scope. Moreover, most were developed before the emergence of generative AI systems.

E. Statutory Law Remedies for Digital and AI-Enabled Harms

In addition to constitutional and data-protection frameworks, South Africa, Nigeria, and Kenya rely on a combination of statutory and common-law remedies to address digital harms involving likeness misuse.

Cybercrime legislation across the three jurisdictions increasingly provides partial protection against AI-enabled image misuse, including deepfakes, synthetic impersonation, and non-consensual dissemination of manipulated content. In South Africa, the Cybercrimes Act 19 of 2020 criminalizes the unlawful distribution of intimate images and other forms of harmful digital communication, thereby capturing certain forms of deepfake pornography and deceptive synthetic media. Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act 2015 similarly addresses online impersonation, identity theft, cyber harassment, and the dissemination of offensive or misleading digital content, provisions capable of applying to AI-generated likeness misuse. In Kenya, the Computer Misuse and Cybercrimes Act 2018 (CMCA) criminalizes cyber harassment, false publication, identity theft, and electronic impersonation, thereby providing indirect remedies against malicious synthetic representations.

However, the Kenyan Computer Misuse and Cybercrimes (Amendment) Act, 2025 significantly expands this framework by strengthening protections against digitally manipulated and deceptive electronic content, including AI-enabled impersonation, falsified digital representations, and technology-facilitated identity abuse. The amendment reflects growing legislative awareness of the risks posed by generative AI systems, particularly in relation to deepfakes, biometric misuse, misinformation, and synthetic identity manipulation.

Additional statutes address specific harms such as revenge pornography, false political information, and obscene content. For example, South Africa's Films and Publications Amendment Act 11 of 2019 and Electoral Act 73 of 1998 may apply to deepfake

pornography and political misinformation respectively; while Nigeria's Violence Against Persons (Prohibition) Act, 2015, and Kenya's Sexual Offences Act, 2024 and Films and Stage Plays Act, 2022 provide partial protection against image-based sexual abuse. In Kenya, the ODPC has issued guidance on the processing of biometric data and the use of facial-recognition technologies, emphasizing consent, purpose limitation, and accountability (Office of the Data Protection Commissioner, 2025).

Although these laws can partially address harms such as defamation, impersonation, and non-consensual sexual imagery, none of these frameworks comprehensively regulate the lifecycle of AI-generated likenesses.

F. AI, Deepfakes, and Emerging Regulatory Responses

Generative AI systems expose significant limitations within existing individual image-rights frameworks across South Africa, Nigeria, and Kenya. Although all three jurisdictions have begun recognizing the regulatory challenges associated with generative AI, synthetic media, and biometric technologies, none currently possesses a comprehensive AI-specific framework governing individual image rights and synthetic identity.

South Africa's National AI Policy Framework acknowledges, for example, concerns relating to privacy, ethics, misinformation, and responsible AI deployment (Department of Communications and Digital Technologies, 2024). However, commentators note that the policy framework remains largely aspirational and innovation-oriented, prioritizing economic growth, digital competitiveness, and AI adoption without establishing comprehensive regulatory rules for generative AI and synthetic identity systems (Fluxmans, 2025). Consequently, important issues relating to AI-generated likenesses remain insufficiently addressed, including biometric scraping, consent for training datasets, ownership and control of synthetic identities, platform accountability, deepfake regulation, and liability for AI-generated impersonation or reputational harm.

Similarly, Nigeria's National AI Strategy (Federal Ministry of Communications, Innovation and Digital Economy [FMCIDE], 2025) and NITDA's Ethical Guidelines for AI (Federal Ministry of Communications, Innovation and Digital Economy [FMCIDE], 2023), and Kenya's CMCA (Amendment) Act, 2025 reflect growing governmental awareness of synthetic identity manipulation, automated decision-making, and algorithmic risk. Nonetheless, the intervention of the ODPC of Kenya in suspending the Worldcoin project in 2023 signals an institutional willingness to constrain AI deployment where consent, transparency, and proportionality are lacking.

Yet these regulatory responses remain incomplete. Although South Africa, Nigeria, and Kenya have begun developing AI governance strategies and digital-policy frameworks, these instruments remain largely policy-oriented, aspirational, or non-binding, with limited enforceable standards governing AI training datasets, biometric scraping, synthetic likeness generation, platform accountability, or consent-based use of personal data. More significantly, existing AI policy frameworks in all three jurisdictions pay insufficient attention to communal cultural interests, indigenous data sovereignty, or the governance of culturally significant imagery within generative AI systems.

G. The Limits of Existing Frameworks in the Age of AI

The comparative experiences of South Africa, Kenya, and Nigeria reveal both convergence and fragmentation in African approaches to individual image rights and communal cultural rights protection. Across these jurisdictions, emerging judicial and legislative developments reflect growing recognition that questions of representation engage broader concerns relating to dignity, likeness, cultural integrity, and social belonging rather than merely commercial value. At the same time, important tensions remain between individual-centered legal doctrines and the relational realities of identity within many African contexts.

These tensions become particularly visible where human representation intersects with communal cultural imagery and traditional cultural expressions which embody both individual identity and collective cultural meaning (UNESCO, 2003; WIPO, 2024; Oguamanam, 2023). Existing legal frameworks continue to regulate personality rights, intellectual property, cultural heritage, and data governance through largely distinct legal regimes, despite increasing recognition that these interests frequently overlap in digital environments (Guadamuz, 2024). Contemporary AI systems further collapse these distinctions by simultaneously processing personal identity, copyrighted works, cultural heritage, and training data within integrated computational processes (Guadamuz, 2024; UNESCO, 2025). As a result, neither individual image-rights doctrines, which primarily protect individual personality and commercial interests, nor existing cultural heritage frameworks, which focus principally on communal cultural preservation, adequately address digital representations that simultaneously implicate identifiable individuals, communal identity, and communal cultural imagery (Kavanagh, 2026; Schulz & Loewen-Colón, 2026).

The emergence of generative AI intensifies this tension. Synthetic media technologies do not simply reproduce images; they transform likeness, cultural aesthetics, and visual identity into data capable of manipulation, recombination, and circulation across digital environments. In doing so, AI systems often detach culturally significant imagery from the social, historical, and spiritual contexts that give such representations meaning within their communities (Ndubisi, 2024). Sacred symbols, ritual imagery, Indigenous aesthetics, and other culturally embedded forms of representation may therefore be digitized, reproduced, repurposed, and commodified in ways that detach them from the cultural relationships, protocols, and spiritual meanings that govern their use, thereby undermining their contextual integrity and cultural significance (WIPO, 2024; Nissenbaum, 2010; Udechukwu, 2026). These developments create regulatory chal-

lenges that extend beyond conventional questions of ownership or publication, requiring legal frameworks to address broader concerns relating to cultural authority, collective consent, communal dignity, and provenance. They also require governance frameworks capable of addressing cultural authority, collective consent, communal dignity, and the governance of identity where individual likeness and communal cultural imagery converge within increasingly automated AI systems (Carroll et al., 2020; Kavanagh, 2026; Schulz & Loewen-Colón, 2026).

Accordingly, the comparative experiences of South Africa, Nigeria, and Kenya suggest that existing legal responses remain conceptually and institutionally insufficient for addressing the relational and technological dimensions of AI-generated representation. By combining personality rights, privacy protections, data governance, cultural heritage protections, and communal consent mechanisms, African legal systems may offer important normative contributions to global debates concerning AI regulation, digital justice, and the governance of identity in the age of AI.

IV. AI AND THE DISRUPTION OF LEGAL AND ETHICAL FRAMEWORKS

Scholars have increasingly observed that generative AI facilitates new forms of cultural extraction and appropriation through the large-scale scraping, replication, and commodification of cultural materials without meaningful consent, attribution, or benefit-sharing (Arya, 2021; Birhane, 2020; Dugeri, 2024; Fitch et al., 2023; WIPO, 2024a; Young, 2008). These concerns are particularly acute in African contexts because inherited Western IP and personality-rights frameworks, which are largely organized around concepts of individual ownership, privacy, and commercial exploitation, inadequately protect communal cultural attributes, Indigenous aesthetics, ritual imagery, and other traditional cultural expressions that embody collective

identity and cultural heritage (Nwauche, 2010; Oguamanam, 2023). Generative AI systems further blur these legal categories by reproducing identifiable persons alongside culturally significant aesthetics, ritual imagery, Indigenous symbols, and communal artistic traditions within the same computational processes, exposing the limitations of legal regimes that continue to regulate personality, intellectual property and cultural heritage as separate domains (Dugari, 2024; Ndubisi, 2024).

Unlike conventional forms of copying, generative AI systems do not usually reproduce images verbatim (Guadamuz, 2024; 2026). Rather, they generate outputs through statistical pattern synthesis, recombining visual features and textual prompts to create representations that evoke recognizable identities, aesthetics, and cultural motifs without replicating a single source image (Guadamuz, 2024; 2026). This process enables AI systems to reproduce culturally distinctive imagery while often falling outside conventional infringement thresholds grounded in originality, fixation, or substantial similarity (Guadamuz, 2024).

The result is a widening gap between existing legal doctrine and the relational, dignitary, and cultural harms experienced by affected individuals and communities. As argued throughout this paper, AI-generated representations may simultaneously implicate both individual image rights and communal cultural interests. Thus, a deepfake of a politician, celebrity, or private citizen primarily concerns personal autonomy, reputation, consent, and identity manipulation. By contrast, the synthetic reproduction of culturally significant attire, sacred symbols, indigenous hairstyles, ritual performances, or traditional aesthetics primarily implicates communal cultural rights, cultural sovereignty, and collective dignity. Increasingly, however, generative AI collapses these categories by reproducing identifiable individuals within culturally significant contexts, thereby implicating both personal and communal interests simultaneously.

These developments raise profound ethical and cultural concerns because AI systems often detach culturally significant

imagery from the social, historical, and spiritual contexts that give such representation their meaning (Ndubisi, 2024; Schulz & Loewen-Colón, 2026). Sacred rituals, ceremonial attire, indigenous hairstyles, and communal artistic expressions may be transformed into decontextualized digital content available for unrestricted circulation, remixing, and commercialization (Fitch et al., 2023; Ndubisi, 2024; Okely, 2025). Here, generative AI does not merely reproduce cultural imagery; it risks stripping culturally significant representations of their social, historical, and spiritual meaning while reinforcing historical patterns of cultural extraction, stereotyping, and epistemic marginalization long associated with colonial systems of knowledge production (Fitch et al., 2023; Kanu and Okpokwasili, 2025).

These dynamics echo historical practices of colonial extraction and cultural exploitation through which indigenous art, rituals, symbols, stories, and bodies were collected, archived, classified, and commodified for external consumption, often without consent or contextual understanding (Boateng, 2011; Metz, 2023; Oguamanam, 2020). Generative AI reproduces this extractive logic under the guise of technological innovation by 'mining' cultural and biometric data in ways that mirror colonial systems of knowledge production and appropriation (Benjamin, 2019; Couldry & Mejias, 2018; 2019). African identities, aesthetics, and cultural expressions become raw material for global AI systems, generating outputs that aestheticize, stereotype, homogenize, and commodify identity for commercial purposes (Birhane, 2020; Fitch et al., 2023; Salami, 2024).

These harms are further exacerbated by machine-vision datasets that reproduce colonial visual hierarchies and racialized classifications. Empirical studies demonstrate that widely used AI datasets often rely on stereotypical, reductive, or poorly contextualized depictions of African and other non-Western communities (Kanu and Okpokwasili, 2025; Salami, 2024). The racialized assumptions embedded within these datasets are subsequently inherited and amplified by generative models, per-

petuating distorted and homogenized representations of marginalized groups (Benjamin, 2019; Crawford & Paglen, 2019). Importantly, these practices bypass the forms of communal consultation and cultural authorization that many African societies require for depictions of sacred ceremonies, cultural symbols, or communal rituals. The result is a form of digital colonialism that perpetuates epistemic and visual dispossession within contemporary AI systems (Fitch et al., 2023; Gausen, 2023; Reed, 2019; Salami, 2024).

A recent Kenyan example illustrates these concerns. In 2024, AI-generated images, reportedly used by the Kenyan State Department of Culture in a public campaign, inaccurately depicted Maasai cultural attire by portraying men wearing the *enkarewa*, a neck ornament traditionally reserved for women (Kasosi, 2025). Within Maasai culture, attire and jewelry function not merely as decorative objects but as markers of age, gender, social status, and spiritual transition. The *Isuri*, for instance, is worn exclusively by older women to symbolize wisdom and authority, while the *Emiragie*, worn by younger women, signifies fertility and vitality. Reassigning these markers arbitrarily disrupts systems of cultural transmission and communal meaning. Such errors exemplify how AI-mediated representation can distort cultural knowledge even in the absence of malicious intent (Kasosi, 2025). The resulting harm, therefore, arose not from misrepresentation of a particular individual's likeness, but from the distortion of communal cultural imagery and culturally embedded systems of meaning.

Comparable concerns arise in other cultural contexts. The APRA AMCOS (2024) report on Aboriginal, Torres Strait Islander, and Māori music documented how generative AI systems distorted Indigenous soundscapes and reproduced culturally sensitive instruments and ceremonial songs outside their appropriate cultural contexts. Participants emphasized that AI-generated reproductions of *taonga pūoro* and *waiata* violated indigenous cultural protocols and called for indigenous-led governance ground-

ed in *tikanga*. Although arising from Australasia, these concerns resonate strongly with African contexts, where cultural expressions similarly embody collective identity, ancestral knowledge, and intergenerational knowledge (Cuthbert, 1998; Dugeri, 2021; Inawat, 2015).

Together, these developments expose significant limitations within existing legal frameworks. Most African image-rights, privacy, and intellectual-property regimes continue to presume identifiable human actors and individualized harms, making them poorly equipped to address AI-generated representations implicating both individual likeness and communal cultural identity simultaneously.

A. Consent and Relational Identity

Consent occupies a central position within African data-protection regimes. Nigeria's Data Protection Act, Kenya's Data Protection Act, and South Africa's POPIA all require informed and voluntary consent for lawful data processing. However, these frameworks generally presume active human participation at the point of data collection and processing. Generative AI complicates this premise by scraping publicly available photographs, biometric identifiers, and visual materials into opaque training datasets without notice, negotiation, or opportunity for withdrawal (Burgess, 2023; Congressional Research Service, 2023).

African philosophies of personhood provide an important normative basis for reimagining consent in this context. Within many African traditions, consent is not understood merely as an isolated individual decision, but as a relational moral act shaped by one's duties to family, lineage, and the community (Akpa-Inyang, & Chima, 2021; Mbiti, 1970). Under Ubuntu, autonomy acquires meaning only when exercised in recognition of its implications for others and for communal harmony (Mokgoro, 1998; Tutu, 1999). This relational understanding implies that decisions concerning the use of likenesses or cultural imagery

therefore implicate not only individual autonomy but also collective dignity and social responsibility.

This relational understanding is reflected in customary governance practices across many African communities, where elders, custodians, lineage heads, or councils participate in decisions concerning photography, recording, or public representation of cultural practices. In many communities, for instance, permission from traditional authorities is required before ceremonies are photographed, oral histories recorded, or traditional attire reproduced, demonstrating that representation is often governed through collective rather than merely individual consent mechanisms (Nwauche, 2015; San Code of Ethics, 2017).

Applied to AI, these principles support a shift away from narrow, individualistic notions of consent toward relational consent frameworks recognizing communities as legitimate rights-bearing stakeholders vis-à-vis common cultural heritage. Such an approach may include community consent boards, cultural-impact assessments, collective licensing structures, and collective authorization protocols for the use of culturally significant imagery in AI systems (Nwauche, 2015). These protocols align closely with the CARE Principles (i.e. Collective Benefit, Authority to Control, Responsibility, and Ethics), which emphasize community authority and ethical stewardship over indigenous and cultural data (Carroll et al., 2020; Walter et al., 2021). Integrating these principles into AI governance frameworks would strengthen resistance to extractive technological practices and support more culturally responsive systems of digital governance.

B. Authorship, Creativity, and Collective Agency

Generative AI also destabilizes traditional understanding of authorship and creativity. Copyright laws in Nigeria, South Africa, and Kenya continue to vest authorship exclusively in human creators (Nigeria Copyright Act 2022, section 2(1); South African Copyright Act, 1978 section 1; Kenya Copyright Act 2001,

section 22). Courts in jurisdictions such as the United Kingdom and China have similarly affirmed that AI systems cannot themselves qualify as legal authors and that protection requires meaningful human intellectual contribution. In *Thaler v Comptroller-General of Patents, Designs and Trademarks* (2023), the English Court of Appeal reaffirmed that authorship must vest in a human creator and that an AI system cannot be recognized as an author. Chinese courts have taken a similar position. In *Shenzhen Tencent v Shanghai Yingxun* (2019), *Li v Liu*, and the *Changshu 'Half-Heart' Case* (2025), courts held that AI-assisted works may receive copyright protection only where a human provides meaningful intellectual input or creative choice; by contrast, the Zhangjiagang Court in 2025 denied protection where human contribution was minimal (Wininger, 2023; China Justice Observer, 2019; IAM Media, 2025; DLA Piper, 2025). Across these decisions, these courts agree that AI may be a tool in the creation of a work, but authorship and the rights that follow remain firmly anchored in human agency.

African relational philosophies offer an alternative perspective rooted in communal creativity and relational agency. Within many African traditions, creativity is understood not as the isolated expression of an autonomous genius, but as an intergenerational and communal process embedded within shared cultural life (Gebru, 2024; Nwauche, 2015). As Mbiti (1970) and Menkiti (1984) observe, personhood, and by extension creative agency, emerges through communal relationships and shared obligations. Ubuntu similarly emphasizes reciprocal knowledge production and socially embedded creativity rather than purely individual authorship (Ramose, 1999; Wiredu, 1996). Together, these demonstrate that creativity in many African contexts is relational and collective rather than wholly individualistic.

From this perspective, AI should be conceptualized as a tool of co-creation rather than an independent rights holder (Shanthi et al., 2025; Yu et al., 2025). African legal systems could, therefore, recognize forms of communal or relational authorship, en-

suring that individuals and communities whose identities, aesthetics, and cultural expressions inform AI outputs retain moral and economic interests grounded in dignity, custodianship, and communal continuity rather than originality alone (Gebru, 2024; Janke 2003).

C. Cultural Representation and Collective Identity

In many African intellectual traditions, cultural representation is inseparable from collective identity. Visual representations depicting people, ceremonies, attire, ritual practices, or cultural objects are not merely depictions of discrete individuals, but expressions of shared history, moral obligation, social belonging, and communal continuity (Mbiti, 1970; Menkiti, 1984; Ramose, 1999; Wiredu, 1996). Theorists such as Gyekye (1997) and Appiah (1994) similarly argue that cultural identity is co-constructed through shared practices, symbols, and representations that sustain collective belonging across generations.

These philosophical assertions have significant implications for image governance. Unlike Euro-American legal frameworks that treat image rights primarily as individual and proprietary interests, African relational philosophies also treat images as socially embedded artifacts implicating communal identity and dignity. Consequently, the distortion, commodification, or unauthorized circulation of culturally significant images may harm not only the depicted individual, but also the broader social fabric of the community itself. This aligns with African customary law and Indigenous data-governance principles, which prioritize communal sovereignty, contextual integrity, collective authorship, and intergenerational stewardship over cultural materials.

Generative AI technologies intensify these risks by enabling the reproduction and circulation of synthetic communal cultural imagery, often detached from its originating context. AI systems trained predominantly by external actors may therefore risk displacing local epistemologies and undermining communal author-

ity over cultural representation. These harms implicate not only cultural accuracy but also collective dignity, self-determination, and cultural sovereignty.

Legal frameworks such as Kenya's Protection of Traditional Knowledge and Cultural Expressions Act (2016) and Nigeria's Copyright Act (2022) partially reflect these communal orientations, although enforcement remains limited. African ethical traditions, nevertheless, provide a more holistic normative framework for cultural-image governance rooted in communal responsibility, relational dignity, and collective stewardship. These perspectives challenge the dominance of purely individualistic models of personality and publicity rights and offer an alternative governance framework grounded in communal sovereignty and relational accountability.

V. RELATIONAL IMAGE GOVERNANCE AND COMMUNAL CULTURAL PROTECTION

As this paper argues in the preceding parts, generative AI increasingly blurs the boundary between individual image rights and communal cultural rights by reproducing identifiable persons alongside culturally significant attire, ritual practices, indigenous aesthetics, sacred symbols, and other traditional cultural expressions. Existing legal frameworks remain ill-equipped to address these overlapping harms. Individual image-rights regimes largely focus on protecting identifiable individuals, while communal cultural rights frameworks protect culturally significant images, symbols, practices, and traditional cultural expressions belonging to or associated with a community. AI-generated representations may combine both, creating a gap in existing legal protection.

This section proposes a relational framework for image governance grounded in African philosophies of personhood, dignity, and communal responsibility. Rather than displacing individual image rights, this framework recognizes that certain forms of

representation may simultaneously implicate personal autonomy and communal cultural identity. It accordingly advances principles of collective custodianship, relational consent, lifecycle governance, and restorative justice as mechanisms for governing culturally significant representations within the context of generative AI and digital cultural reproduction.

A. Indigenous and Comparative Models of Cultural Image Governance

The increasing digitization of cultural materials and the expansion of generative AI have intensified global debates concerning Indigenous Data Sovereignty (IDSov). IDSov frameworks broadly assert that Indigenous peoples and communities should retain authority over the collection, storage, governance, and use of data relating to their identities, heritage, and cultural expressions (Kukutai & Taylor, 2016; Snipp, 2016). These concerns become significant where photographs and other visual representations depicting ceremonial practices, traditional attire, sacred symbols, and culturally embedded imagery are incorporated into machine-learning systems without meaningful community participation, free, prior and informed consent, attribution, or equitable benefit-sharing (Longpre et al., 2024; Christen & Anderson, 2019; Morgera, 2022; Schulz & Loewen-Colón, 2026).

African legal systems have not yet developed comprehensive legal frameworks specifically regulating the use of communal cultural imagery in AI contexts, notwithstanding emerging regional initiatives on AI and Indigenous knowledge governance (African Union, 2024). Nevertheless, normative guidance may be drawn from IDSov scholarship and comparative Indigenous governance models in jurisdictions such as Australia, Canada, and New Zealand with more developed IDSov systems, which conceptualize culturally significant data as subject to collective custodianship, collective authority, and relational responsibility rather than exclusive individual ownership (Walter & Carroll, 2020; Kukutai & Cormack, 2020, pp. 24, 28-29). This article does not suggest that the legal experiences from these jurisdictions

should be transplanted into African legal systems, nor does it imply that Indigenous communities across these jurisdictions share identical historical, constitutional or cultural experiences. Rather, these jurisdictions are mentioned because they have developed legal and governance responses to questions of collective cultural authority, Indigenous knowledge governance, community consent and the management of culturally significant data in the digital environment.

These approaches recognize that increasing datafication and digitalization create both new opportunities and new forms of data colonialism, reinforcing the need for governance frameworks that preserve Indigenous self-determination and community authority over culturally significant imagery (Kukutai & Cormack, 2020, p. 24; Kavanagh, 2026). Consistent with this approach, UNESCO has emphasized that AI governance should respect cultural diversity, Indigenous knowledge systems and meaningful community participation, suggesting that IDSov principles provide a persuasive normative foundation for regulating communal cultural imagery in AI systems (UNESCO, 2021; UNESCO, 2025).

A leading example is Canada's OCAP® framework (Ownership, Control, Access, and Possession), developed by the First Nations Information Governance Centre (FNIGC, 2014). OCAP® principles affirm that First Nations retain collective authority over all forms of community-related data, including photographs, digitized archives, and other visual cultural materials, by recognizing their rights to determine how such materials are collected, accessed, managed, used, and shared (FNIGC, 2014). Similarly, in Aotearoa, New Zealand, Māori governance framework grounded in *tikanga Māori* regulates the reproduction and circulation of culturally significant imagery depicting *taonga* such as carved ancestral figures, *tukutuku* panels, *tā moko*, portraits of *tūpuna*, and *wāhi tapu* (Mead, 2003). The Wai 262 Report further affirms Māori guardianship (*kaitiakitanga*) over cultural materials and supports Māori authority in decisions concerning

reproduction, digitization, and commercialization of cultural materials (Waitangi Tribunal, 2011).

These principles are increasingly extended into digital and AI governance through initiatives such as *Te Mana Raraunga* (Māori Data Sovereignty Network), which advocates culturally informed metadata systems, controlled access protocols, and *iwi* guardianship over visual and cultural data (Kukutai & Taylor, 2016). Australia's Indigenous Cultural and Intellectual Property (ICIP) framework similarly recognizes collective custodianship over indigenous cultural imagery and emphasizes free, prior, and informed consent, alongside equitable benefit-sharing, for culturally significant representations (Fitch et al., 2023; Janke, 2025a; 2025b; Okely, 2025). These frameworks demonstrate how IDSov principles can be translated into concrete governance mechanisms that safeguard cultural authority throughout the data lifecycle. It therefore provides a useful comparative model for developing governance frameworks capable of protecting communal cultural imagery within African AI ecosystems.

Comparable approaches exist across African contexts. Among the Maasai of Kenya and Tanzania, the Maasai Intellectual Property Initiative seeks to formalize community authority over the commercial use of Maasai names, attire, and cultural imagery through collective governance structures capable of negotiating licenses, monitoring use, and challenging exploitative appropriation (Afro-IP, 2017; Maasai Intellectual Property Initiative, n.d.). Similarly, the San Code of Research Ethics (2017) establishes community-based protocols governing photography, visual documentation, and representation in research settings, emphasizing fairness, consultation, feedback, and benefit-sharing. The Code further recognizes community interests in the storage, dissemination, and contextualization of culturally sensitive visual materials (South African San Institute, 2017).

Among the Himba communities of Namibia, customary norms and community leadership structures continue to regulate photography, tourism imagery, and media representations

involving culturally significant appearance, attire, and ritual identity. Although these governance mechanisms remain less formalized, Himba communities have increasingly challenged exploitative stock-photo commercialization, sought contextualization of culturally sensitive imagery, and resisted forms of representation detached from local cultural meaning (The Namibian, 2012). Recent controversies surrounding the moderation of images depicting traditional dress further illustrate tensions between global digital-platform standards and local cultural understandings of representation and dignity (Columbia University Global Freedom of Expression, 2025).

Collectively, these examples demonstrate that governance of culturally significant imagery frequently centers on custodianship, communal authority, relational responsibility, and cultural sovereignty, rather than on purely proprietary or individualistic conceptions of ownership (IP Australia & Terri Janke and Company, 2018; Janke, 1998). At the same time, their effectiveness remains constrained by jurisdictional fragmentation, the territorial nature of intellectual property protection, and a continued reliance on formal documentation systems that inadequately capture the living, evolving, and performative character of cultural practices and other forms of intangible cultural heritage (WIPO, 2024; UNESCO, 2025, p. 25; Oguamanam, 2023). These limitations are particularly significant in AI contexts, where culturally significant imagery and knowledge may be detached from their cultural context and transformed into machine-readable datasets that fail to reflect the dynamic and community-based nature of Indigenous cultural expression (Udechukwu, 2026; Kavanagh, 2026; Schulz & Loewen-Colón, 2026). Consequently, many forms of Indigenous and communal cultural expression remain vulnerable to digital appropriation, decontextualization, and algorithmic extraction within contemporary AI systems, as existing governance frameworks often fail to preserve community authority, cultural context, and provenance throughout the AI lifecycle (Ndubisi, 2024; Udechukwu, 2026).

Nevertheless, these frameworks provide important normative foundations for developing more context-sensitive approaches to governing AI-generated likenesses and communal cultural imagery within African contexts. The CARE Principles are particularly relevant because they emphasize collective benefit, community authority, responsibility, and ethical governance of Indigenous data across the data lifecycle (Carroll et al., 2020). However, their application to generative AI raises a further question: how should responsibility be addressed when a user generates culturally significant images from an AI system? Requiring every user to obtain community consent would be impractical, while consent at the training stage may not address subsequent harms such as cultural expropriation, misrepresentation, or misalignment. Thus, while the CARE Principles provide a useful normative foundation, they do not determine how responsibility should be allocated for AI-generated outputs.

B. Ubuntu Relational Personhood and Image Governance

The Ubuntu philosophy of personhood provides an important normative framework for rethinking image governance where individual likeness intersects with communal cultural identity. Rather than conceiving identity as an autonomous attribute of the individual, Ubuntu understands personhood as constituted through relationships of mutual recognition, reciprocity, and communal belonging, such that individual identity is realized within, rather than independent of, the community (Gyekye, 1997; Mbiti, 1970; Menkiti, 1984; Metz, 2011; Ramose, 1999). This relational conception of personhood provides a compelling normative foundation for recognizing rights in communal cultural imagery, particularly where representations embody shared cultural values, collective memory or traditional cultural expressions (Ajitoni, 2024; Kavanagh, 2026). Representation therefore carries social and moral significance extending beyond the individual depicted, particularly where images embody shared cultural meanings, communal memory, spirituality, or collective identity.

Viewed from this lens, communal cultural rights emerge as a natural extension of existing personality, publicity, and individual image rights doctrines; complementing rather than replacing existing individual image-rights frameworks. The objective is not to subordinate individual image rights to communal control, but to develop layered governance mechanisms capable of recognizing situations in which likeness and communal cultural rights overlap. This need is increasingly evident in efforts by African communities to challenge the unauthorized commercial exploitation of communal cultural imagery. The Maasai Intellectual Property Initiative, for example, reclaimed community authority over the unauthorized commercial use of Maasai names, attire, and cultural representation (Afro-IP, 2017; Brindle & Florman, 2021; Livni, 2016). Comparable efforts by the Zulu nation to challenge exploitative commercialization of Zulu cultural identity similarly reflect growing demands for legal frameworks capable of recognizing communal interests in communal cultural imagery (Afro-IP, 2017).

These developments suggest the need for governance frameworks extending beyond conventional IP and personality-rights models. Building on international cultural heritage law, Indigenous data governance, and AI governance scholarship, communal cultural-image governance may be understood as a governance framework that recognizes the collective interests of indigenous peoples and local communities in the protection, authorization, contextualization, and circulation of communal cultural imagery that embody communal identity, heritage, spiritual values or traditional cultural expression (UNGA, 2007, arts. 11, 31–32; UNESCO, 2003; WIPO, 2024; Oguamanam, 2023). It affirms that decisions concerning the creation, digitization, use and reuse of such representations should be informed not only by individual consent but also by community governance, cultural protocols and the continuing authority of the communities to which they belong (Christen & Anderson, 2019; Carroll et al., 2020; Kavanagh, 2026). Such an approach draws from broader principles of

collective custodianship already reflected in traditional cultural expression regimes, IDSov frameworks, cultural-heritage protections, and instruments such as the African Charter for Cultural Renaissance (2006) and the United Nations Declaration on the Rights of Indigenous Peoples (2007). However, it extends these principles into the governance of living and embodied representations, including communal cultural likenesses and AI-generated imagery. In the AI context, this framework further requires that communal cultural imagery remain connected to its cultural provenance and contextual meaning throughout the AI lifecycle, thereby preserving the contextual integrity of such representations and reducing the risks of decontextualization, cultural misappropriation, and AI extractivism (Nissenbaum, 2010; Udechukwu, 2026; Schulz & Loewen-Colón, 2026).

Importantly, these communal cultural rights need not displace individual image rights. Both may coexist within a layered framework of protection, in which individual image rights safeguard personal autonomy, dignity, and privacy, while communal cultural rights preserve cultural integrity, contextual meaning, and collective identity. Such an approach aligns closely with the African Charter on Human and Peoples' Rights (1981), which recognizes both individual dignity and collective cultural entitlements under Articles 17 and 22. More broadly, embedding relational and communal approaches within image governance contributes to wider efforts to decolonize intellectual-property and digital-governance frameworks by recognizing African philosophies of personhood, cultural sovereignty, and communal responsibility within the regulation of AI-generated representation and digital identity.

C. Governance Principles for Relational Image and Cultural Representation

A workable African framework for governing AI-generated likeness and communal cultural imagery should rest on four interrelated governance principles: collective custodianship, rela-

tional consent, lifecycle governance, and restorative justice with equitable benefit-sharing. These principles do not create absolute communal ownership over identity or likeness. Rather, they provide governance mechanisms for situations where representations implicate communal cultural rights, heritage, spirituality, or traditional cultural expressions.

1. Collective custodianship

Collective custodianship recognizes that communities may possess legitimate interests in communal cultural imagery linked to communal identity, heritage, or spirituality. This principle aligns closely with the CARE Principle of Authority to Control, which affirms community authority over cultural and indigenous data. Under this approach, communities function as custodians of communal cultural imagery. This custodianship may extend to ceremonial attire, sacred imagery, ritual practices, communal aesthetics, or culturally significant symbols reproduced within AI systems or digital platforms (FNIGC, 2014; Janke, 2025a; 2025b; San Ethics, 2017).

This principle is increasingly reflected in instruments such as the Swakopmund Protocol, the United Nations Declaration on the Rights of Indigenous Peoples (UNGA, 2007), the UNESCO Convention for the Safeguarding of Intangible Cultural Heritage (2003), and domestic frameworks governing indigenous knowledge and traditional cultural expressions. Judicial developments such as *Milpurrurru v Indofurn* similarly demonstrate growing recognition that misuse of culturally significant imagery may inflict communal cultural harm in addition to economic loss (Janke, 1995).

2. Relational consent (FPIC+)

Relational consent extends beyond narrow individualistic notions of consent by recognizing that representations involving communal cultural imagery may require forms of collective consultation or authorization alongside individual permission.

Within many African traditions, decisions concerning representation are shaped by obligations to family, lineage, and community rather than by purely atomistic autonomy (Nwauche, 2017). This approach aligns with broader indigenous principles of Free, Prior, and Informed Consent (FPIC), while grounding consent within African traditions of relational responsibility and communal accountability (IP Australia & Terri Janke and Company, 2018; Janke, 2025a; 2025b).

Practically, the governance of culturally significant imagery in AI systems should therefore be informed by principles of collective or relational consent, recognizing that where such imagery embodies communal identity, heritage or spiritual significance, decisions concerning its digitization and reuse may engage collective as well as individual interests. Drawing on the principle of FPIC reflected in the United Nations Declaration on the Rights of Indigenous Peoples (UNGA, 2007) and the Nagoya Protocol, relational consent acknowledges that legitimate authorization may require engagement with the representative institutions through which communities exercise authority over their cultural heritage, including elders, cultural custodians, or other recognized governance structures before culturally significant imagery is incorporated into AI systems, digitized archives, or commercial projects (UNGA, 2007, Articles 18, 32; Oguamanam, 2023; Kavanagh, 2026).

For AI systems, this supports a collective consent mechanism under which developers or other actors seeking to collect, digitize, scrape, or incorporate culturally significant material into training datasets engage with authorized community representatives before such use occurs (Carroll et al., 2020; Kyi et al., 2026; Sridhar, 2020). Such a mechanism would avoid requiring individual users to obtain consent for every AI-generated image while enabling communities to establish conditions concerning attribution, permissible uses, commercial exploitation, and culturally inappropriate representations. Kenya's *Protection of Traditional Knowledge and Cultural Expressions Act, 2016* provides

a useful African example of community authority over traditional knowledge and cultural expressions. The Act recognizes communities' rights to control and protect their traditional knowledge and cultural expressions, including the right to authorize their exploitation and to prevent specified forms of use without prior informed consent. It also empowers owners to grant authorization for their exploitation and use, thereby placing community consent at the center of the legal framework governing access to and use of these forms of cultural heritage (Protection of Traditional Knowledge and Cultural Expressions Act, 2016, ss. 10(1), 18(2), 23(2), 25(1)).

However, the availability of cultural material online should not, by itself, be treated as consent to its incorporation into AI systems. This is particularly important where digitisation and online dissemination may expose traditional cultural expressions to uses beyond those authorised by the communities concerned (WIPO, 2023). Nigerian jurisprudence provides a useful analogy. In *Ndidi-Amaka Odogwu v Quilox Restaurant & Bar Ltd* (2017) and *Adunni Adewale v Polanc Media Ltd* (2025), the courts rejected the proposition that the online availability of an individual's image amounted to consent to its subsequent use. Although these cases concern individual image rights, they support the broader principle that online accessibility does not extinguish consent requirements.

Importantly, this approach does not displace individual autonomy but supplements it where communal cultural imagery is implicated. This understanding is consistent with African communitarian thought, which recognizes that individual rights are exercised within a network of reciprocal relationships and shared responsibilities rather than in isolation (Gyekye, 1997; Ikuenobe, 2018b). This is illustrated by the San Code of Research Ethics, which requires researchers to engage with recognized community governance structures before undertaking research involving photographs, recordings or other culturally significant materials. By recognizing that consent must be obtained through

legitimate community institutions as well as from individual participants where appropriate, the Code demonstrates how relational consent can be operationalized in ways that respect both individual autonomy and collective cultural stewardship (South African San Institute, 2017; Carroll et al., 2020; Schulz & Loewen-Colón, 2026).

3. Lifecycle data governance

Effective governance of AI-generated cultural imagery requires authority across the entire data lifecycle rather than solely at the point of collection or consent. Communities should therefore retain meaningful oversight concerning digitization, metadata creation, storage, dataset inclusion, AI training, downstream reuse, and deletion of culturally significant imagery (Carroll et al., 2020, 2021).

Under an Ubuntu-informed communal image-rights framework, effective communal image rights require authority not only at the point of consent but across the entire data lifecycle (San Code of Ethics, 2017). African communities should retain oversight over the digitization, metadata creation, access controls, inclusion in AI training datasets, and downstream uses of communal cultural imagery, reflecting the principles of Indigenous data governance that recognize continuing community authority throughout the data lifecycle (Christen & Anderson, 2019; Carroll et al., 2020; UNESCO, 2025). This could be in the form of collective consent at the upstream stages of data collection and AI training, where developers or other entities responsible for the data engage authorised community representatives and establish conditions governing access, attribution, permissible uses, commercial exploitation, and deletion (Carroll et al., 2021; Kyi et al., 2026; Sridhar, 2020). Once these conditions are established, individual users will not ordinarily require separate consent for each prompt. Where, however, an AI-generated output involves sacred, restricted, or otherwise culturally sensitive imagery, additional safeguards should apply to ensure that the

output does not violate the conditions established by the relevant community.

Consequently, AI-generated representations of culturally significant attire, rituals, or oral traditions should be accompanied by provenance metadata identifying their origin, cultural significance, applicable usage restrictions, and community protocols, thereby ensuring that cultural meaning and custodial obligations remain attached to digital representations rather than being lost through technological reuse (Christen & Anderson, 2019; Longpre et al., 2024; Udechukwu, 2026). Without such governance, communal cultural imagery risks being decontextualized, misrepresented, and transformed into digital assets detached from their social relationships, cultural norms, and systems of authority that give them meaning, perpetuating the forms of AI extractivism identified in recent scholarship (Kavanagh, 2026; Nissenbaum, 2010; Schulz & Loewen-Colón, 2026).

This principle aligns with emerging international frameworks including the African Union Data Policy Framework (2022) and UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021), both of which emphasize community participation, transparency, and responsible digital governance.

In AI contexts, lifecycle governance is particularly important because opacity in training datasets and model development often obscures how culturally significant imagery is sourced, transformed, and repurposed (Dugari, 2024; Guadamuz, 2024; UNESCO, 2025). The reliance of foundation models on large-scale, under-documented datasets makes it difficult to trace provenance, verify consent, and determine whether culturally significant images have been acquired and used in accordance with the norms, expectations, and cultural protocols of the communities from which they originate (Longpre et al., 2024; UNESCO, 2021). This lack of transparency undermines accountability and increases the risk of unauthorized appropriation, decontextualization and the erosion of community authority over cultural materials. Accordingly, provenance should extend beyond iden-

tifying an image's technical source to documenting its cultural provenance through governance mechanisms that require provenance disclosure and culturally informed metadata recording the cultural significance of imagery, applicable restrictions, attribution requirements and community expectations governing its reuse (Christen & Anderson, 2019; Udechukwu, 2026). Such an approach reflects Udechukwu's (2006) proposal for culturally contextual datasheets and Christen & Anderson's (2019) work on metadata and Traditional Knowledge (TK) Labels, which seek to preserve cultural context and communicate continuing community authority over cultural materials despite their digitization. These measures should be complemented by community-defined usage protocols that empower Indigenous peoples and local communities to determine the conditions under which culturally significant imagery may be accessed, used and reused throughout the AI lifecycle. This approach is consistent with emerging scholarship on AI extractivism, which advocates meaningful community participation, free, prior and informed consent, equitable benefit-sharing and continuing community authority over AI data governance and aligns with UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021) and the CARE Principles for Indigenous Data Governance (Carroll et al., 2020). Viewed in this way, lifecycle governance constitutes a normative framework for preserving the contextual integrity of culturally significant imagery by ensuring that the cultural relationships, responsibilities and systems of authority attached to such imagery continue to govern its collection, digitization, use and reuse within AI systems.

By embedding lifecycle control within communal cultural rights, African legal systems can move beyond reactive remedies toward proactive governance, one that prevents misappropriation, supports ethical curation, and ensures that digital and AI technologies operate in ways consistent with communal dignity and cultural sovereignty.

4. Restorative justice and equitable benefit-sharing

The final principle concerns restorative justice and equitable benefit-sharing. African traditions frequently prioritize repair, reconciliation, and restoration of dignity rather than purely punitive remedies (Akpa-Inyang, & Chima, 2021; Mokgoro, 1998; Tutu, 1999). Within an Ubuntu-informed framework, the unauthorized use of communal cultural imagery, particularly through AI systems, should trigger remedies that address both material loss and symbolic harm.

Equitable benefit-sharing constitutes a practical manifestation of restorative justice (De Jonge, 2011; Morgera, 2016). Where communal cultural imagery generates economic, reputational, or technological value, communities must share in those benefits. This principle also aligns with international benefit-sharing frameworks such as the Nagoya Protocol on Access and Benefit-Sharing (2010), the WIPO Treaty on Intellectual Property, Genetic Resources and Associated Traditional Knowledge (2024b), and broader indigenous data-sovereignty approaches recognizing that communities should share in the value generated from their cultural expressions and representations.

Consequently, this principle will require that AI developers, platforms, researchers, and cultural institutions actively mitigate foreseeable harms and engage in culturally respectful practices throughout the lifecycle of image use. This includes ongoing consultation, culturally competent governance mechanisms, and responsiveness to community concerns even after deployment (San Code of Ethics, 2017). Failure to do so perpetuates extractive dynamics and reproduces digital colonialism (Salami, 2024).

By institutionalizing restorative justice and equitable benefit-sharing within this framework, African AI governance can move beyond defensive protection toward transformative justice. Such an approach ensures that technological innovation contributes to cultural continuity, empowerment, and self-representa-

tion rather than reinforcing historical patterns of dispossession (Oguamanam, 2019; 2020). In doing so, it embeds dignity, reciprocity, and collective responsibility at the heart of image governance in the digital age.

D. Operationalizing Communal Cultural Image Governance in the AI Era

Operationalizing communal cultural image governance requires institutional, procedural, and technological mechanisms capable of translating these normative principles into enforceable governance structures.

1. Legal and institutional architecture

One important mechanism would involve statutory recognition of communal cultural rights and interests in communal cultural imagery within data-protection, intellectual property, cultural-heritage, and AI-governance frameworks. Consequently, operationalizing interests in communal cultural imagery requires a multilayered governance framework that combines legal reform with meaningful community participation and culturally grounded regulatory mechanisms (Ndubisi, 2024, p. 174; UNESCO, 2025, paras. 171–173). Such a framework would recognize that formal intellectual property rules alone are insufficient to protect communal cultural rights and must be complemented by participatory decision-making, customary governance institutions, and regulatory processes that respect the cultural values, authority, and self-determination of affected communities (Kavanagh, 2026; Oguamanam, 2020; UNGA, 2007, Art. 18, 31, 32).

One important approach may involve extending principles of communal custodianship into digital environments through community image protocols. Like the San community protocols, these protocols would allow communities to define the conditions under which communal cultural imagery may be photographed, digitized, reproduced, or incorporated into AI systems. Commu-

nities could, for example, prohibit commercial use of sacred rituals, ceremonial performances, or culturally sensitive imagery without prior community authorization. The Swakopmund Protocol similarly demonstrates that African legal frameworks can recognize collective interests in cultural expressions, providing a useful foundation for regulating AI-generated cultural imagery.

States may also adopt *sui generis* protections or amend intellectual-property, cultural-heritage, and data-protection laws to recognize communal cultural rights. Such frameworks require community authorization before communal cultural images are digitized, publicly disseminated, or incorporated into AI training datasets, while also imposing attribution and benefit-sharing obligations. Community claims may further be recorded in cultural registries or clearinghouses like India's Traditional Knowledge Digital Library (TKDL) (Janke, 2025a; 2025b; Udechukwu, 2026) for traditional knowledge.

Data-protection frameworks may likewise recognize forms of collective data subjecthood where communal cultural imagery implicates communal identity and heritage. This approach aligns with broader Indigenous Data Sovereignty principles emphasizing community authority over data connected to collective identity and traditional knowledge (Carroll et al., 2020; Kukutai & Taylor, 2016; Oguamanam, 2019).

Institutional mechanisms such as community consent boards and cultural registries could further record customary protocols, permissions, and licensing conditions governing communal cultural imagery. Integrating machine-readable metadata into these systems would assist archivists, digital platforms, and AI dataset curators in respecting culturally defined access and usage conditions (Christen & Anderson, 2019; Udechukwu, 2026).

Transparency obligations for AI developers are equally important. Developers should be required to disclose the provenance and composition of training datasets, particularly where

communal cultural imagery or identifiable persons are involved. Such measures align with broader calls for dataset accountability in response to racialized bias, algorithmic opacity, and extractive data practices embedded within AI systems (Crawford & Paglen, 2019; Udechukwu, 2026).

Likewise, African states and communities should support community-based licensing and governance structures capable of negotiating with AI developers and administering benefit-sharing arrangements. The Maasai Intellectual Property Initiative provides an important example of how communities may reclaim governance authority over communal cultural imagery through coordinated licensing and collective representation mechanisms (Afro-IP, 2017; Brindle & Florman, 2021).

At the continental level, the African Union could further strengthen these protections by embedding communal cultural-image governance principles within the African Union Continental AI Strategy (2024) and reinforcing them through complementary instruments such as the Charter for African Cultural Renaissance (2006) and the African Union Data Policy Framework (2022). Together, these frameworks would help advance Africa's cultural sovereignty within increasingly transnational digital ecosystems while promoting more equitable and culturally responsive approaches to AI governance.

2. Protecting cultural data sovereignty in the age of generative AI

Protecting cultural data sovereignty in the age of generative AI requires governance frameworks that recognize the collective dimensions of identity, representation, and cultural heritage within many African and Indigenous communities (Janke, 2025a). Existing AI governance models remain largely focused on individual privacy and commercial innovation, often overlooking the communal and cultural implications of AI-generated representations (Nweke, 2024). Emerging African governance initiatives therefore increasingly emphasize the need for cultur-

ally grounded and context-sensitive approaches to AI regulation (African Union Continental AI Strategy, 2024, para 2.1-2.2, ps. 27-28; Ndubisi, 2024).

The African Declaration on Artificial Intelligence (2025), for example, calls for AI systems to reflect 'Africa's strategic priorities, shared values, and diverse cultural contexts'. Building on this principle, AI governance frameworks should require developers to engage directly with affected communities when collecting, digitizing, or synthesizing culturally identifiable imagery. In contexts involving communal cultural images, principles of Free, Prior, and Informed Consent may therefore need to extend beyond individual consent to encompass forms of collective consultation and community authorization (Janke, 2025a; 2025b). Equally important is the inclusion of African artists, cultural custodians, and indigenous knowledge holders within AI governance processes to ensure that technological systems respect local cultural norms and avoid extractive forms of representation (Janke, 2025a; 2025b).

Mandatory Cultural Impact Assessments (CIAs) could provide a practical mechanism for identifying and mitigating cultural harm before AI systems are deployed. Rather than creating overly burdensome approval processes, CIAs may operate as targeted risk-assessment tools triggered only where AI systems utilize communal cultural imagery, indigenous cultural materials, or community-linked datasets. Similar to environmental or data-protection impact assessments, developers would be required to evaluate issues such as provenance of training data, consent procedures, risks of stereotyping or cultural distortion, and potential benefit-sharing obligations (Udechukwu, 2026; UNESCO, ICCROM, ICOMOS, & IUCN, 2022).

To ensure practical implementation, CIAs could be administered through existing national data-protection authorities, AI ethics committees, or cultural agencies, with community consultation required only in contexts involving culturally sensitive imagery or identifiable communal representations. This approach

would enable regulators to identify high-risk uses of communal cultural imagery without imposing blanket restrictions on AI development. Scholars increasingly argue that such targeted assessments are necessary to address emerging forms of digital and algorithmic colonialism associated with generative AI systems (Birhane, 2020; Kanu & Okpokwasili, 2025; Salami, 2024). By integrating CIAs at the AI project-design stage, policymakers and developers can anticipate forms of cultural harm that conventional privacy or copyright frameworks routinely overlook, ensuring alignment with community-defined values, consent practices, and governance norms.

Operationalizing these safeguards nevertheless requires institutional mechanisms capable of translating communal interests into enforceable governance structures. AI developers using communal cultural imagery should therefore engage directly with affected communities through mechanisms such as community consent boards responsible for determining whether and how cultural imagery may be digitized or incorporated into AI training datasets (San Code of Research Ethics, 2017). National AI ethics bodies should likewise include cultural experts, traditional authorities, and indigenous knowledge custodians to ensure that governance decisions reflect culturally informed perspectives.

E. Continental Coordination and African AI Governance

Finally, effective governance of AI-generated likeness and communal cultural imagery ultimately requires continental coordination and normative harmonization. Given the transnational nature of generative AI systems, isolated domestic regulation is unlikely to provide adequate protection against cross-border extraction, circulation, and commercial exploitation of communal cultural imagery.

The African Union therefore has an important role to play in embedding culturally grounded and relational approaches

to image governance within emerging continental AI and digital-governance frameworks. Through the African Union Continental AI Strategy (2024, para 2.4.1; Table 1, pgs. 22-23), the African Charter for Cultural Renaissance (2006, articles 3, 4(c), 21, 22, 26), and the African Union Data Policy Framework (2022, para 2.1), the African Union has already committed itself to developing harmonized, Africa-centered governance frameworks that promote ethical AI, safeguard digital rights, preserve African cultural values and support inclusive digital transformation. Embedding governance principles that recognize communal interests in communal cultural imagery would therefore be a natural extension of these continental initiatives.

Importantly, such coordination should not merely replicate Western models of publicity rights or data governance. As this paper argues, African legal and philosophical traditions offer important normative resources for rethinking image governance in contexts where representation implicates both individual dignity and communal cultural identity. Principles of relational personhood, communal responsibility, custodianship, and restorative justice may therefore provide more context-sensitive approaches to AI-generated likenesses and culturally significant imagery within plural and culturally diverse societies.

Ultimately, the challenge posed by generative AI is not solely technological or doctrinal. It is also philosophical and ethical. As AI systems increasingly transform likeness and cultural imagery into globally circulating digital commodities, African legal systems face the task of developing governance frameworks capable of protecting both individual autonomy and communal cultural rights without collapsing one into the other.

VI. CONCLUSION

The intersection of generative AI, individual image rights, and Indigenous African cultural expressions reveals deep ten-

sions between technological innovation and longstanding struggles for cultural justice. While generative AI offers new possibilities for cultural preservation, creativity, and visibility, it also risks reproducing extractive and colonial patterns when deployed without culturally grounded safeguards. African philosophical traditions that prioritize relationality and respect, particularly Ubuntu, provide an essential counterpoint to these risks by reframing likeness as a relational good; images are not merely individual attributes or technical inputs but expressions of communal identity, moral worth, and intergenerational belonging.

Embedding these insights into law, policy, and AI governance requires a shift from individualistic to communal models of image rights. Such an approach demands statutory recognition of communal cultural rights, procedural mechanisms for collective consent, transparent data provenance, Cultural Impact Assessments, and enforceable benefit-sharing regimes. It also calls for coordinated action at the continental level, ensuring that African Union institutions play an active role in harmonizing standards and safeguarding cultural sovereignty.

By grounding digital governance in Ubuntu and related normative commitments, Africa can reclaim agency in shaping its technological and cultural future. This framework transforms digital innovation into a vehicle for empowerment, self-representation, and cultural affirmation, rather than a continuation of historical patterns of extraction. In the age of generative AI, protecting communal dignity and cultural-image sovereignty is not only a legal challenge but a moral imperative that affirms Africa's right to define, represent, and protect its identities on its own terms.

REFERENCES

Abacha v. Fawehinmi, 6 NWLR (Pt. 660) 228 (S.C.) (2000).

Abdulsalam, A., Nkume, D., & Osilesi, O. (2025). *No consent, no use: How the Quilox decision strengthens image rights protection in Nigeria*. PUNUKA Attorneys & Solicitors. https://punuka.com/wp-content/uploads/2025/11/no-consent-no-use-article-final.pdf

Adewale v. Polance Media Ltd. & Fadoju, LD/17781MFHR/2024 (High Court of Lagos State, June 24, 2025).

Africa Check. (2023). *No, video does not show Nigerian traditional leader using human head, but a figurine used in cultural festival*. https://africacheck.org/fact-checks/meta-programme-fact-checks/no-video-does-not-show-nigerian-traditional-leader-using

African Declaration on Artificial Intelligence. (2025). *Africa Declaration on Artificial Intelligence*. https://cdn.prod.website-files.com/601987a724bdae251872ed2c/685038b76606772aa2b3f90e_Africa-Declaration-on-Artificial-Intelligence.pdf

African Regional Intellectual Property Organization. (2010). *Swakopmund Protocol on the Protection of Traditional Knowledge and Expressions of Folklore*. https://www.aripo.org/

African Union. (1981). *African Charter on Human and Peoples' Rights*. https://au.int/en/treaties/african-charter-human-and-peoples-rights

African Union. (2006). *Charter for African Cultural Renaissance*. https://au.int/en/treaties/charter-african-cultural-renaissance

African Union. (2022). *African Union data policy framework*. https://au.int/en/documents/20220728/african-union-data-policy-framework

African Union. (2024). *Continental artificial intelligence strategy: Harnessing AI for Africa's development and prosperity*. https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy

Afriklens. (2024, November 1). *African hairstyles: Cultural significance and legacy*. Retrieved October 15, 2025, from https://www.afriklens.com/african-hairstyles-cultural-significance-and-legacy/

Afriquei Noir Magazine. (2025, May 16). *The red crown: Himba women's hair*. Retrieved October 15, 2025, from https://afriquenoirmagazine.com/the-red-crown-himba-womens-hair/

Afro-IP. (2017, February 3). *Zulu and Maasai nations spearhead TK initiatives*. Retrieved October 14, 2025, from https://afro-ip.blogspot.com/2017/02/zulu-and-maasai-nations-spearhead-tk.html

Ahonsi, V. (2024, April 5). *Scarification of the Dinka tribe: A cultural tradition and symbol of beauty*. I Love Africa. Retrieved October 30, 2025, from https://iloveafrica.com/scarification-of-the-dinka-tribe/

Akpa-Inyang, F., & Chima, S. C. (2021). South African traditional values and beliefs regarding informed consent and limitations of the principle of respect for autonomy in African communities: A cross-cultural qualitative

study. *BMC Medical Ethics, 22*(1), 111. https://doi.org/10.1186/s12910-021-00678-4

Al-Sibai, N. (2024, January 8). OpenAI pleads that it can't make money without using copyrighted materials for free. *Futurism*. Retrieved October 21, 2025, from https://futurism.com/the-byte/openai-copyrighted-material-parliament

Allsobrook, C. J. (2023). African recognition of dignity as a basis for universal human rights. *Acta Academica, 55*(1). https://doi.org/10.38140/aa.v55i1.7268

Amazing and Wonderful. (2024). *The hair rituals of the Himba people: A deep dive into cultural significance, styling techniques, and materials used*. Retrieved October 03, 2025, from https://amazingandwonderful.com/the-hair-rituals-of-the-himba-people-a-deep-dive-into-cultural-significance-styling-techniques-and-materials-used/

Ani, A. (2026, March 10). *Sabinus' "Something Hooge": PCCSIGN boss settles ₦1bn, ₦100m trademark disputes with Peak Milk, Gala. The Sun*. retrieved August 19, 2026, from https://thesun.ng/sabinus-something-hooge-pccsign-boss-settles-n1bn-n100m-trademark-disputes-with-peak-milk-gala/

Andersen v. Stability AI Ltd., No. 3:23-cv-00201 (N.D. Cal. Jan. 13, 2023).

Ann Njoki Kumena v. KTDA Agency Ltd., Civil Case No. 7 of 2015 [2019] eKLR.

APRA AMCOS. (2024). *AI and music*. Retrieved October 16, 2025, from https://www.apraamcos.com.au/about/supporting-the-industry/research-papers/aiandmusic

Appiah, K. A. (1994). Identity, authenticity, survival: Multicultural societies and social reproduction. In A. Gutmann (Ed.), *Multiculturalism* (pp. 149–164). Princeton University Press.

Aremu, P., Banjo, B., & Olanipekun, O. (2012). Egungun tradition in trado-modern society in South-Western Nigeria. *Mediterranean Journal of Social Sciences, 3*(1), 283–291. https://doi.org/10.5901/mjss.2012.03.01.283

Arya, R. (2021). Cultural appropriation: What it is and why it matters? *Sociology Compass, 15*(6), e12923. https://doi.org/10.1111/soc4.12923

Asia IP. (2023, February 28). *The face of image rights*. Retrieved October 5, 2025, from https://asiaiplaw.com/section/in-depth/the-face-of-image-rights

Atoyebi, O. M. (2024, April 14). *Image rights in Nigeria: A legal perspective*. *The Nigeria Lawyer*. Retrieved October 30, 2025, from https://thenigerialawyer.com/image-rights-in-nigeria-a-legal-perspective/

Ayalew, Y. E. (2024). An old question in a new domain: Some preliminary insights on balancing the right to privacy and freedom of expression in the digital era under African human rights law. In L. A. Abdulrauf & H. Dube (Eds.), *Data privacy law in Africa: Emerging perspectives* (pp. 79–103). Pretoria University Law Press.

Babalola, O. (2022). Nigeria's data protection legal and institutional model: An overview. *International Data Privacy Law, 12*(1), 44–52. https://doi.org/10.1093/idpl/ipab023

Benjamin, R. (2019). *Race after technology: Abolitionist tools for the New Jim Code*. Polity Press.

Birhane, A. (2020). Algorithmic colonization of Africa. *SCRIPTed, 17*(2), 389–409. https://doi.org/10.2966/scrip.170220.389

Birhane, A. (2021). Algorithmic injustice: A relational ethics approach. *Patterns, 2*(2), 1–9.

Blackshaw, I. (2019). *Understanding sports image rights*. World Intellectual Property Organization. Retrieved October 15, 2025, from https://www.wipo.int/en/web/ipday/2019/understanding_sports_image_rights

Blundell, G. (1998). Some aspects concerning rock art and national identity in South Africa. In *Proceedings of the Khoisan identities and cultural heritage conference* (pp. 153–156). University of the Western Cape.

Boateng, B. (2011). *The copyright thing doesn't work here.* University of Minnesota Press.

Brindle, M., & Florman, N. (2021). The Maasai intellectual property initiative: A 20th-century model for turning assets into income. *Journal of Fair Trade, 2*(2), 5–12. https://doi.org/10.13169/jfairtrade.2.2.0005

Burgess, M. (2023, April 4). *ChatGPT has a big privacy problem*. *Wired*. Retrieved October 30, 2025, from https://www.wired.com/story/italy-ban-chatgpt-privacy-gdpr/

Catherine Njeri Wanjiru v. Machakos University, Petition E021 of 2021 [2022] KEHC 10599 (KLR) (Aug. 3, 2022)

Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J., Anderson, J., & Hudson, M. (2020). The CARE principles for Indigenous data governance. *Data Science Journal, 19*, Article 43. https://doi.org/10.5334/dsj-2020-043

Carroll, S. R., Garba, I., Figueroa-Rodríguez, O. L., Holbrook, J., Lovett, R., Materechera, S., Parsons, M., Raseroka, K., Rodriguez-Lonebear, D., Rowe, R., Sara, R., Walker, J. D., Anderson, J., & Hudson, M. (2021). Operationalizing the CARE and FAIR principles for Indigenous data futures. *Scientific Data, 8*, Article 108. https://doi.org/10.1038/s41597-021-00892-0

Carroll, S. R., & Walter, M. (2020). Indigenous data sovereignty, governance and the link to Indigenous policy. In M. Walter, T. Kukutai, S. R. Carroll, & D. Rodriguez-Lonebear (Eds.), *Indigenous data sovereignty and policy* (pp. 1–20). Routledge.

Changshu 'Half-Heart' case. (2025). *China IP Law Update*. Retrieved May 12, 2026, from https://www.chinaiplawupdate.com/2025/03/chinese-court-again-rules-there-is-copyright-in-ai-generated-images/

Chen, J., & Friedmann, D. (2025, February). Protecting sacred art and identity: From intellectual property to traditional cultural expressions. *Harvard International Law Journal*. https://journals.law.harvard.edu/ilj/2025/02/

China Justice Observer. (2019). *Chinese court backs copyrights for AI-created*

works. Retrieved October 30, 2025, from https://www.chinajusticeobserver.com/

Chisam. (2024). *Exploring Igbo tribal marks: Types and their cultural significance*. OgbonoBlog. Retrieved October 28, 2025, from https://ogbonoblog.com/igbo-trends/exploring-igbo-tribal-marks-types-and-their-cultural-significance/

Christen, K., & Anderson, J. (2019). Toward slow archives. *Archival Science, 19*(2), 87–116;

Columbia University Global Freedom of Expression. (2025). *Oversight Board cases of images of partially nude Indigenous women*. Retrieved October 15, 2025, from https://globalfreedomofexpression.columbia.edu/cases/oversight-board-cases-of-images-of-partially-nude-indigenous-women/

Computer Misuse and Cybercrimes Act, No. 5 of 2018 (Kenya).

Congressional Research Service. (2023). *Generative artificial intelligence and data privacy: A primer* (CRS Report No. R47569). Retrieved October 18, 2025, from https://crsreports.congress.gov/product/pdf/R/R47569

Consumer Protection Act 68 of 2008 (South Africa).

Constitution of the Federal Republic of Nigeria 1999, Cap. C23, Laws of the Federation of Nigeria.

Constitution of the Republic of South Africa 1996 (South Africa) (Act 108 of 1996).

Convention on Biological Diversity. (2011). *Nagoya Protocol on access to genetic resources and the fair and equitable sharing of benefits arising from their utilization to the Convention on Biological Diversity: Text and annex*. Secretariat of the Convention on Biological Diversity.

Copyright Act, Cap. 130 (Kenya).

Copyright Act 2022 (Nigeria) (Act No. 8 of 2022)

Cornelius, S. (2008). Image rights in South Africa. *International Sports Law Journal, 3–4*, 71–88.

Cornelius, S. (2011). Commercial appropriation of a person's image. *Potchefstroom Electronic Law Journal, 14*(2), 184–199.

Cornelius, S. (2024). *Sports image rights: Legal protection in South Africa and Kenya*. *Sports Law & Taxation*.

Coronel, P., & Coronel, M. (n.d.). San peoples create earliest African art. In *Great events from history: The ancient world* (pp. 1–3). Salem Press.

Couldry, N., & Mejias, U. A. (2019). Data colonialism: Rethinking big data's relation to the contemporary subject. *Television & New Media, 20*(4), 336–349. https://doi.org/10.1177/1527476418796632

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

3Cuthbert, D. (1998). Beg, borrow or steal: The politics of cultural appropriation. *Postcolonial Studies, 1*(2), 257–262.

Cybercrimes (Prohibition, Prevention, etc.) Act, 2015 (Nigeria).

Cybercrimes Act 19 of 2020 (South Africa).

Department of Communications and Digital Technologies. (2024). *South Africa national artificial intelligence policy framework: Towards the development of South Africa national artificial intelligence policy*. https://www.dcdt.gov.za/sa-national-ai-policy-framework/file/338-sa-national-ai-policy-framework

Data Protection Act No. 24 of 2019 (Kenya).

De Jonge, B. (2011). What is fair and equitable benefit-sharing? *Journal of Agricultural and Environmental Ethics, 24*(2), 127–146. https://doi.org/10.1007/s10806-010-9249-3

Disney Enterprises, Inc. v. Midjourney, Inc., No. 2:25-cv-05275 (C.D. Cal. filed June 11, 2025).

DLA Piper. (2025, March 21). *Another Chinese court finds that AI-generated images can be protected by copyright: The Changshu People's Court and the "Half Heart" case*. JD Supra. https://www.jdsupra.com/legalnews/another-chinese-court-finds-that-ai-2389042/

Dogan, S. L., & Lemley, M. A. (2006). What the right of publicity can learn from trademark law. *Stanford Law Review, 58*(4), 1161–1220. https://www.jstor.org/stable/40040289

Drewal, M. T. (1992). *Yoruba ritual: Performers, play, agency*. Indiana University Press.

Dugeri, M. (2024). The cannibalization of culture: Generative AI and the appropriation of Indigenous African musical works. *Journal of Intellectual Property and Information Technology Law, 4*(1), 17–67. https://doi.org/10.52907/jipit.v4i1.502

Edema, T., & Ecoma, B. E. (2024). Advocating for image right protection through the lens of history. *Journal of Private and Property Law, 21*(1), 113–123.

Electronic Communications and Transactions Act 25 of 2002 (South Africa).

Electoral Act 73 of 1998 (South Africa).

Emerging Market Telecommunication Services v. Barr Godfrey Nya Eneye, (2018) LPELR-46193 (Nigeria).

Federal Ministry of Communications, Innovation and Digital Economy. (2023). *Ethical guidelines for artificial intelligence in Nigeria.*

Federal Ministry of Communications, Innovation and Digital Economy. (2025, September). *National artificial intelligence strategy*. National Centre for Artificial Intelligence and Robotics.https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf

Films and Publications Amendment Act 11 of 2019 (South Africa).

Films and Stage Plays Act, Cap. 222 (Kenya).

Fitch, E., McKenzie, C., Janke, T., & Shul, A. (2023, November 30). *The new frontier: Artificial intelligence, copyright and Indigenous culture*. Terri Janke and Company.

Fluxmans. (2025, June 10). *AI regulation in South Africa: Legal gaps & progress*. Retrieved October 25, 2025, from https://www.fluxmans.com/article/

ai-regulation-south-africa

Fuente, J. A. (2003). Protecting the rights of Indigenous cultures under the current intellectual property system. *The John Marshall Review of Intellectual Property Law, 3*(1), 88–102.

Gbadegesin, S. (1991). *African philosophy: Traditional Yoruba philosophy and contemporary African realities*. Peter Lang.

Gebru, A. K. (2024). Communal authorship. *University of Richmond Law Review, 58*(2), 337–388.

Gelias LLP. (2025). *Navigating the thin line between image rights and copyright*. Retrieved May 17, 2026, from https://www.gelias.com/images/Image_Right_v_Copyright.pdf

Getty Images (US), Inc. & Ors v. Stability AI Ltd., [2025] EWHC 2863 (Ch).

George Washington University Law School. (2025). *AI litigation database*. Retrieved January 10, 2026, from https://blogs.gwu.edu/law-eti/ai-litigation-database/

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press. https://www.deeplearningbook.org/contents/ml.html

Grütter v. Lombard and Another, 2007 (4) SA 89 (SCA).

Guadamuz, A. (2017). Artificial intelligence and copyright. *WIPO Magazine*. Retrieved October 14, 2024, from https://www.wipo.int/en/web/wipo-magazine/articles/artificial-intelligence-and-copyright-40141

Guadamuz, A. (2024). A scanner darkly: Copyright liability and exceptions in artificial intelligence inputs and outputs. *GRUR International, 73*(2), 111–127. https://doi.org/10.1093/grurint/ikad140

Guadamuz, A. (2026). *Dr Andres Guadamuz—Written evidence (AIC0026).* House of Lords Communications and Digital Select Committee inquiry: *AI and copyright*. UK Parliament. https://committees.parliament.uk/writtenevidence/162681/html/

Gyekye, K. (1996). Person and community in Akan thought. In K. Wiredu & K. Gyekye (Eds.), *Person and community* (pp. 101–122). The Council for Research in Values and Philosophy.

Gyekye, K. (1997). *Tradition and modernity: Philosophical reflections on the African experience*. Oxford University Press.

Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866 (2d Cir. 1953).

Hayes, C. M. (2023). *Generative artificial intelligence and copyright: Both sides of the black box* (SSRN Scholarly Paper No. 4517799). Social Science Research Network. Retrieved October 15, 2025, from https://ssrn.com/abstract=4517799

Himonga, C., Taylor, M., & Pope, A. (2013). Reflections on judicial views of Ubuntu. *Potchefstroom Electronic Law Journal, 16*(5).

IAM Media. (2025). *Chinese court denies copyright protection for AI-generated content where human input is insufficient*. Retrieved May 16, 2026, from https://www.iam-media.com/article/chinese-court-denies-copyright-pro-

tection-ai-generated-content-insufficient-human-input-in-first-of-its-kind-ruling

Ikuenobe, P. (2006). *Philosophical perspectives on communalism and morality in African traditions*. Lexington Books.

Ikuenobe, P. (2018a). An examination of Menkiti's conception of personhood and Gyekye's critique. In E. Etieyibo (Ed.), *Method, substance, and the future of African philosophy*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-70226-1_10

Ikuenobe, P. (2018b). Radical versus moderate communitarianism: Gyekye's and Matolino's misinterpretations of Menkiti. *Filosofia Theoretica: Journal of African Philosophy, Culture and Religions*, *7*(2), 79–100. https://doi.org/10.4314/ft.v7i2.6

Inawat, R. J. (2015). Music as cultural heritage. *The John Marshall Review of Intellectual Property Law, 14*, 228–250.

Intellectual Property Office—Guernsey Registry. (n.d.). *Image rights*. Guernsey Registry. Retrieved November 21, 2025, from https://ipo.guernseyregistry.com/article/3929/image-rights

IOL. (2024, February 14). *SA law fails to protect people's image rights*. *IOL Cape Times*. Retrieved October 15, 2025, from https://iol.co.za/capetimes/news/2024-02-14-sa-law-fails-to-protect-peoples-image-rights/

IP Australia, & Terri Janke and Company. (2018). *Indigenous knowledge: Issues for protection and management*. IP Australia.

Janke, T. (1995). Briefs: Copyright—The carpet case. *Aboriginal Law Bulletin, 3*(72), 36. https://classic.austlii.edu.au/au/journals/AboriginalLawB/1995/13.html

Janke, T. (1998). *Our culture, our future: Report on Australian Indigenous cultural and intellectual property rights*. Michael Frankel & Company.

Janke, T. (2003). *Minding culture: Case studies on intellectual property and traditional cultural expressions*. World Intellectual Property Organization. https://www.wipo.int/edocs/pubdocs/en/tk/781/wipo_pub_781.pdf

Janke, T. (2025a, August 11). *AI got no dreaming: Defending Indigenous rights in the digital age*. Terri Janke & Company. https://www.terrijanke.com.au/post/ai-got-no-dreaming-defending-indigenous-rights-in-the-digital-age

Janke, T. (2025b, August 14). *Keeping our data strong: Upholding Indigenous data sovereignty through data sharing agreements*. Terri Janke & Company. https://www.terrijanke.com.au/post/keeping-our-data-strong-upholding-indigenous-data-sovereignty-through-data-sharing-agreements

Jessicar Wanjiru v. Davinci Aesthetics & Reconstruction Centre & 2 Others, [2017] KEHC 9230 (KLR) (Constitutional Petition No. 410 of 2016).

Kahaka, M., & Maundeni, W. (2022). Comparing some traditional Western and African conceptions of personhood. *European Journal of Humanities and Social Sciences, 2*(5), 57–62. https://doi.org/10.24018/ejsocial.2022.2.5.308

Kang'ara, S. W. (2011). Why take private law seriously in Africa? *American University International Law Review, 26*(4), 1125–1152. Retrieved October

29, 2025, from https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1725&context=auilr

Kanu, I. A., & Okpokwasili, O. A. (2025). Artificial intelligence and digital colonialism in Africa. *Igwebuike: An African Journal of Arts and Humanities, 11*(7), 2–13.

Karras, T., Aittala, M., Laine, S., Härkönen, E., Hellsten, J., Lehtinen, J., & Aila, T. (2021). *Alias-free generative adversarial networks*. arXiv. https://doi.org/10.48550/arXiv.2106.12423

Kasosi, L. (2025, August 8). Indigenous peoples and AI: Defending rights, shaping the future of technology. *Cultural Survival*. Retrieved October 10, 2025, from https://www.culturalsurvival.org/news/indigenous-peoples-and-ai-defending-rights-shaping-future-technology

Kavanagh, E. (2026). Pluralistic AI governance: Indigenous knowledge and the right of Indigenous peoples to self-determination. *AI & Society, 41*, 6421–6432. https://doi.org/10.1007/s00146-026-02938-6

Kenyatta, J. (1965). *Facing Mount Kenya*. Vintage.

Kumalo v. Cycle Lab (Pty) Ltd., (31871/2008) [2011] ZAGPJHC 56 (17 June 2011).

Kleinhans, M.-M., & Macdonald, R. A. (1997). What is a critical legal pluralism? *Canadian Journal of Law and Society, 12*(2), 25–46.

Kquofi, S., Amate, P., & Tabi-Agyei, E. (2013). Symbolic representation and socio-cultural significance of selected Akan proverbs in Ghana. *Research on Humanities and Social Sciences, 3*(1), 86–98. https://www.iiste.org/Journals/index.php/RHSS/article/view/4101

Kukutai, T., & Taylor, J. (2016). Data sovereignty for indigenous peoples: Current practice and future needs. In T. Kukutai & J. Taylor (Eds.), *Indigenous data sovereignty: Toward an agenda* (pp. 1–22). ANU Press. https://doi.org/10.22459/CAEPR38.11.2016

Kukutai, T., & Cormack, D. (2020). 'Pushing the space': Data sovereignty and self-determination in Aotearoa New Zealand. In M. Walter, T. Kukutai, S. R. Carroll, & D. Rodriguez-Lonebear (Eds.), *Indigenous data sovereignty and policy* (pp. 21–43). Routledge https://doi.org/10.4324/9780429273957

Kuria v. University of Kabianga, Petition E002 of 2022, [2023] KEHC 809 (KLR) (Feb. 10, 2023).

Kyi, L., Gölz, P., Berjon, R., & Biega, A. J. (2026). From clicks to consensus: Collective consent assemblies for data governance. *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems*, Article 348, 1–17. https://doi.org/10.1145/3772318.3790690;

La Salle, M., & Commodifications of Cultural Heritage Working Group. (2014). *Appropriation and commodification of cultural heritage: Ethical and intellectual property issues to consider* [Fact sheet]. Intellectual https://www.sfu.ca/ipinch/sites/default/files/resources/fact_sheets/ipinch_commodificationfactsheet_final.pdf

Lawal-Arowolo, A. (2015). *Losing their status: Traditional peoples in Africa, their intellectual properties and laws* (SSRN Scholarly Paper No. 2694904). Social Science Research Network. https://doi.org/10.2139/ssrn.2694904

Li v. Liu, (Jing 0491 Min Chu No. 11279, Beijing Internet Court, 2023). Retrieved May 12, 2026, from https://english.bjinternetcourt.gov.cn/pdf/BeijingInternetCourtCivilJudgment112792023.pdf

Livni, E. (2016, October 11). The Maasai want their brand back. *Quartz*. Retrieved October 15, 2025, from https://qz.com/896520/the-maasai-want-their-brand-back

Logeais, D., & Schroeder, J. (1998). The French right of image: An ambiguous concept protecting the human personality. *Loyola of Los Angeles Entertainment Law Journal, 9*, 511–536.

Longpre, S., Mahari, R., Obeng-Marnu, N., Brannon, W., South, T., Gero, K. I., Pentland, A., & Kabbara, J. (2024). Position: Data authenticity, consent, & provenance for AI are all broken: What will it take to fix them? In *Proceedings of the 41st International Conference on Machine Learning* (Vol. 235, pp. 32711–32725). PMLR. https://proceedings.mlr.press/v235/longpre24b.html

Lorenz, P., Perset, K., & Berryhill, J. (2023). *Initial policy considerations for generative artificial intelligence*. Organisation for Economic Co-operation and Development. https://doi.org/10.1787/fae2d1e6-en

Lumumba, P. L. O. (2023). The imperative of ubuntu in contemporary judicial decision-making: A case for the utility of ubuntu in understanding rights. In *Ubuntu in the age of human rights* (pp. 1–28). LexisNexis Rule of Law Foundation. https://www.lexisnexisrolfoundation.org/pdf/ubuntu-in-the-age-of-human-rights.pdf

Maasai Intellectual Property Initiative. (n.d.). *Frequently asked questions*. Retrieved October 04, 2025, from https://maasaiintellectualpropertyinitiative.org/

Mangope, K., & Alberts, W. (2022). 'Something old, something new': Aspects of personality rights in the United States and South Africa. *Obiter, 43*(3), 1–20. from https://www.scielo.org.za/pdf/obiter/v43n3/01.pdf

Matolino, B., & Kwindingwi, W. (2013). The end of Ubuntu. *South African Journal of Philosophy, 32*(2), 197–205. https://doi.org/10.1080/02580136.2013.817637

Mbiti, J. S. (1970). *African religions and philosophy*. Anchor Books.

McCarthy, J. T., & Schechter, R. E. (2023). *The rights of publicity and privacy* (2nd ed.). Thomson Reuters.

McGinty, B. (n.d.). *Himba hair rituals*. Infringe. Retrieved on October 15, 2025, from https://www.infringe.com/himba-hair-rituals/

McMullan, J., & Stasiuk, G. (2025, March 12). How AI images are 'flattening' Indigenous cultures—creating a new form of tech colonialism. *The Conversation*. https://theconversation.com/how-ai-images-are-flattening-indigenous-cultures-creating-a-new-form-of-tech-colonialism-246972

Mead, H. M. (2003). *Tikanga Māori: Living by Māori values*. Huia Publishers.

Menkiti, I. A. (1984). Person and community in African traditional thought. In R. A. Wright (Ed.), *African philosophy: An introduction* (3rd ed., pp. 171–181). University Press of America.

Metz, T. (2011). Ubuntu as a moral theory and human rights in South Africa. *African Human Rights Law Journal, 11*(2), 532–559. https://hdl.handle.net/10520/EJC51951

Milpurrurru v. Indofurn Pty Ltd., (1994) 54 FCR 240 (Federal Court of Australia).

Mokgoro, Y. (1998). Ubuntu and the law in South Africa. *Buffalo Human Rights Law Review, 4*(1), 15–25. https://digitalcommons.law.buffalo.edu/bhrlr/vol4/iss1/3/

Morgera, E. (2016). The need for an international legal concept of fair and equitable benefit-sharing. *European Journal of International Law, 27*(2), 353–383. https://doi.org/10.1093/ejil/chw014

Mostert, F., & Cruz, S. (2023). Perspectives on international image rights over the past twenty years. In H. Bosher & E. Rosati (Eds.), *Developments and directions in intellectual property law: 20 years of The IPKat* (pp. 161–192). Oxford University Press. https://doi.org/10.1093/oso/9780192864475.003.0011

Mudasiru, W. (2022). Explainer: What Sabinus' lawsuit means for creators and their intellectual property. *Culture Custodian*. Retrieved November 02, 2025, from https://culturecustodian.com/explainer-what-sabinus-lawsuit-means-for-creators-and-their-intellectual-property/

Mutuku Ndambuki Matingi v. Rafiki Microfinance Bank Limited, [2021] KEHC 9059 (KLR) (High Court at Machakos, Kenya).

Navajo Nation v. Urban Outfitters, Inc., 935 F. Supp. 2d 1147 (D.N.M. 2013).

Ndidi-Amaka Odogwu v. Quilox Restaurant & Bar Ltd., No. FHC/L/CS/482/2017 (Federal High Court of Nigeria, Lagos Judicial Division).

Ndubisi, E. J. O. (2024). Artificial intelligence and the management of African cultural heritage: Towards economic growth and development. *Journal of African Studies and Sustainable Development, 7*(5), 170–183. https://www.apas.africa/journal_article.php?j=jassd-590

Netsheria. (2021). *Protection of image rights in Kenya*. Retrieved October 23, 2025, from https://netsheria.com/protection-of-image-rights-in-kenya/

Nigeria Data Protection Act, 2023, No. 37 (Nigeria).

Nimmer, M. B. (1954). The right of publicity. *Law and Contemporary Problems, 19*(2), 203–223. https://scholarship.law.duke.edu/lcp/vol19/iss2/6/

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nnaemeka, J. (2023). *A critical discourse on African communalism vis-a-vis Western individualism: The existential realities*. SSRN. Retrieved July 12, 2026, from https://doi.org/10.2139/ssrn.4424478

Nwabueze, S. A., & Olumekor, T. (2021, August 18). *Beyond the runway: Understanding the scope of image rights protection under Nigerian law*. International Bar Association. Retrieved January 10, 2024, from https://www.ibanet.org/image-rights-protection-nigerian-law

Nwali v. Ebonyi State Independent Electoral Commission (EBSIEC) & Ors., (2014) LPELR-23682(CA).

Nwauche, E. S. (2015). The emerging right to communal intellectual property. *Marquette Intellectual Property Law Review, 19*(2), 221–249. https://scholarship.law.marquette.edu/iplr/vol19/iss2/4

Nwauche, E. (2017). *The protection of traditional cultural expressions in Africa*. Springer. https://doi.org/10.1007/978-3-319-57231-4

Nweke, N. E. (2024). AI ethics in Africa: Balancing innovation with cultural and social responsibilities. *Iconic Research and Engineering Journals, 8*(3), 451–460. https://www.irejournals.com/paper-details/1706316

Nyerere, J. K. (1968). *Ujamaa: Essays on socialism*. Oxford University Press.

Office of the Data Protection Commissioner. (2025). *Guidance note on biometric data*. https://www.odpc.go.ke/wp-content/uploads/2025/11/ODPC-%E2%80%93-Guidance-Note-on-Biometric-Data.pdf

Ofosu-Asare, Y. (2025). Cognitive imperialism in artificial intelligence: Counteracting bias with Indigenous epistemologies. *AI & Society, 40*, 3045–3061. https://doi.org/10.1007/s00146-024-02065-0

Ogbah, I. O., Odunaike, D. A., & Olugasa, O. (2026). Image rights protection: A comparative analysis of legal frameworks in selected jurisdictions. *African Journal of Law, Ethics and Education, 9*(2), 207–227. https://ajlee-journal.com/index.php/ajlee/article/view/327

Ogonjo, F. A. (2023, March 1). *Legal protections for image rights in Kenya*. Centre for Intellectual Property and Information Technology Law (CIPIT). https://cipit.strathmore.edu/legal-protections-for-image-rights-in-kenya/

Oguamanam, C. (2006). *International law and Indigenous knowledge: Intellectual property, plant biodiversity, and traditional medicine*. University of Toronto Press.

Oguamanam, C. (2019). *Indigenous data sovereignty: Retooling Indigenous resurgence for development* (CIGI Paper No. 234). Centre for International Governance Innovation. https://www.cigionline.org/publications/indigenous-data-sovereignty-retooling-indigenous-resurgence-development/

Oguamanam, C. (2020). Indigenous peoples, data sovereignty, and self-determination: Current realities and imperatives. *The African Journal of Information and Communication, 26*, 1–20. https://doi.org/10.23962/10539/30360

Oguamanam, C. (2023). A critical examination of the African legal framework for Indigenous knowledge. *Journal of African Law, 67*(1), 1–21. https://doi.org/10.1017/S0021855323000049

O'Keeffe v. Argus Printing and Publishing Co Ltd., 1954 (3) SA 244 (C).

Oke, E. K. (2020). Image rights and passing off: Should reputation be enough for celebrities to succeed in English courts? *Journal of Intellectual Property Law & Practice, 15*(1), 49–54. https://doi.org/10.1093/jiplp/jpz143

Okediji, R. L. (2018). *Traditional knowledge and the public domain* (CIGI Paper No. 176). Centre for International Governance Innovation. https://www.cigionline.org/publications/traditional-knowledge-and-public-domain/

Okely, R. (2025, April 17). *The problem with AI-generated images*. Arts Law Centre of Australia. https://www.artslaw.com.au/the-problem-with-ai-generated-images/

Olubiyi, I. A., Adaji, A. E., & Adetula, A. F. (2020). Increasing the commercial value of image rights in Nigeria: Legal possibilities. *Journal of Intellectual Property Law & Practice, 15*(3), 193–197. https://doi.org/10.1093/jiplp/jpz177

Oluwadamilola Banire v. NTA-Star TV Network Limited, (2021) LPELR-52824(CA).

OpenAI. (2023, December 5). *Written evidence (LLM0113)* [Written evidence]. House of Lords Communications and Digital Select Committee. https://committees.parliament.uk/writtenevidence/126981/pdf/

Orie, Ọ. O. (2011). The structure and function of Yoruba facial scarification. *Anthropological Linguistics, 53*(1), 15–33. https://doi.org/10.1353/anl.2011.0000

Oyiwona, R. U. (2025). Importance of the protection of expression of folklore to the society. *Journal of Customary and Religious Law, 2*(2), 54–59. https://journals.unizik.edu.ng/jocarl/article/view/6478

Port Elizabeth Municipality v. Various Occupiers, (2004) CCT 53/03 [2004] ZACC 7.

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383–423. https://doi.org/10.15779/Z383J3C

Protection of Personal Information Act 4 of 2013 (South Africa).

Protection of Traditional Knowledge and Cultural Expressions Act, Cap. 218A (2016) (Kenya).

Protection, Promotion, Development and Management of Indigenous Knowledge Act 6 of 2019 (South Africa).

Radford, A., Kim, J. W., Hallacy, C., Ramesh, A., Goh, G., Agarwal, S., Sastry, G., Askell, A., Mishkin, P., Clark, J., Krueger, G., & Sutskever, I. (2021). Learning transferable visual models from natural language supervision. In *Proceedings of the 38th International Conference on Machine Learning* (Vol. 139, pp. 8748–8763). PMLR. https://proceedings.mlr.press/v139/radford21a.html

Ramose, M. B. (1999). *African philosophy through Ubuntu*. Mond Books.

Reed, T. G. (2021). Fair use as cultural appropriation. *California Law Review, 109*(4), 1373–1442. https://doi.org/10.15779/Z38V97ZS35

Rombach, R., Blattmann, A., Lorenz, D., Esser, P., & Ommer, B. (2021). *High-resolution image synthesis with latent diffusion models* [Preprint]. arXiv. https://doi.org/10.48550/arXiv.2112.10752

Rothman, J. E. (2018a). *The right of publicity: Privacy reimagined for a public world*. Harvard University Press.

Rothman, J. E. (2018b). *The right of publicity: Privacy reimagined for New York?* [Faculty scholarship]. University of Pennsylvania Carey Law School. https://scholarship.law.upenn.edu/faculty_scholarship/2406

Sag, M. (2024). Fairness and fair use in generative AI. *Fordham Law Review, 92*(5), 1887–1921. https://ir.lawnet.fordham.edu/flr/vol92/iss5/7/

Salami, A. O. (2024). Artificial intelligence, digital colonialism, and Africa's future. *Data & Policy, 6*, e67. https://doi.org/10.1017/dap.2024.75

Samuelson, P. (2023). AI authorship? *Communications of the ACM, 66*(3), 24–26. https://cacm.acm.org/opinion/ai-authorship/

Schulz, M., & Loewen-Colón, J. (2026). Preventing AI extractivism: The case for braiding Indigenous data justice with ABS for stronger AI data governance. *AI & Society*. Advance online publication. https://doi.org/10.1007/s00146-026-02931-z

Segun, S. (2024). Are certain African ethical values at risk from artificial intelligence? *Data & Policy, 6*, e68. https://doi.org/10.1017/dap.2024.64

Senghor, L. S. (1964). *On African socialism* (M. Cook, Trans.). Praeger.

SERAP v. Federal Republic of Nigeria, ECW/CCJ/JUD/40/22 (Community Court of Justice of the Economic Community of West African States, July 14, 2022). Retrieved October 12, 2025, from https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2022/08/twitter-final.pdf

Sexual Offences Act, No. 3 of 2006 (Kenya) (as amended).

Shanthi, V., Palanimurugan, P., & Bharathi, M. T. (2025). Artificial intelligence as a co-creative tool for writing screenplays. *Academic Research Journal of Science and Technology (ARJST), 2*(3), 14–27. https://publications.ngmc.ac.in/journal/index.php/arjst/article/view/92

Snipp, C. M. (2016). What does data sovereignty imply: What does it look like? In T. Kukutai & J. Taylor (Eds.), *Indigenous data sovereignty: Toward an agenda* (pp. 39–55). ANU Press. https://doi.org/10.22459/CAEPR38.11.2016

South African San Institute. (2017). *San code of research ethics*. https://www.globalcodeofconduct.org/wp-content/uploads/2025/08/San-Code-of-RESEARCH-Ethics-Booklet_English.pdf

Sridhar, S. (2020, December 2). *Collective consent for algorithmic accountability: The need to rethink the individualistic framework of 'informed' consent*. Institute for Internet and the Just Society. https://www.internetjustsociety.org/collective-consent-for-algorithmic-accountabilitybaaa8d68

S v. Makwanyane and Another, [1995] ZACC 3.

Swenson, G. (2018). Legal pluralism in theory and practice. *International Studies Review, 20*(3), 438–462. https://doi.org/10.1093/isr/viy006

Synodinou, T. (2014). Image right and copyright law in Europe: Divergences and convergences. *Laws, 3*(2), 181–207. https://doi.org/10.3390/laws3020181

Takim, A. O., & Ozim, M. C. (2025). Pragmemes of Ekpe cult rites. *LASU Postgraduate School Journal, 2*(2). https://doi.org/10.5281/zenodo.17053582

Tariemi, O. (2022, May 30). *Skit maker Sabinus sues Peak for using trademark "Something Hooge"*. *The Guardian Nigeria*. Retrieved October 12, 2025, from https://guardian.ng/life/skit-maker-sabinus-sues-peak-for-using-trademark-something-hooge/

Tencent v. Yingxun Tech, (2019) Yue 0305 Min Chu 14010 (Shenzhen Nanshan District People's Court). Retrieved May 12, 2026, from https://www.chinajusticeobserver.com/law/x/2019-yue-0305-min-chu-14010

Thaler v. Comptroller-General of Patents, Designs and Trademarks, [2023] EWCA Civ 1010.

First Nations Information Governance Centre. (2014, May). *Ownership, control, access and possession (OCAP™): The path to First Nations information governance*. https://fnigc.ca/wp-content/uploads/2020/09/5776c4ee9387f966e6771aa93a04f389_ocap_path_to_fn_information_governance_en_final.pdf

The Namibian. (2012, November 28). *Zemba, Himba demonstrate over exclusion*. Retrieved October 12, 2025, from https://www.namibian.com.na/zemba-himba-demonstrate-over-exclusion/

Trademarks Act, Cap. T13, Laws of the Federation of Nigeria 2004.

Tsebee, D., & Oloyede, R. (2024, November 6). *DPAs and AI regulation in Africa*. International Association of Privacy Professionals. https://iapp.org/news/a/dpas-and-ai-regulation-in-africa

Tutu, D. (1999). *No future without forgiveness*. Doubleday.

Ubom v. Globacom (Nig.) Ltd., 6 NWLR (Pt. 1985) 157 (2025).

Udechukwu, L. M. (2026). Culturally contextual datasheets: A framework for embedding cultural reflexivity in global AI governance. *AI and Ethics, 6*, Article 231. https://doi.org/10.1007/s43681-026-01069-4

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2003). *Convention for the safeguarding of the intangible cultural heritage*.

United Nations Educational, Scientific and Cultural Organization (UNESCO). (2021). *Recommendation on the ethics of artificial intelligence*.

UNESCO, ICCROM, ICOMOS, & IUCN. (2022). *Guidance and toolkit for impact assessment in a World Heritage context*. UNESCO World Heritage Centre. https://whc.unesco.org/en/guidance-toolkit-impact-assessments/

UNESCO. (2025). *Report of the Independent Expert Group on Artificial Intelligence and Culture (CULTAI Independent Expert Group Report).*

United Nations. (1948). *Universal Declaration of Human Rights*.

United Nations. (1966). *International Covenant on Economic, Social and Cultural Rights*.

United Nations General Assembly. (2007). *United Nations Declaration on the Rights of Indigenous Peoples* (A/RES/61/295). https://www.un.org/development/desa/indigenouspeoples/declaration-on-the-rights-of-indigenous-peoples.html

Van Gensen, L. I. (2023). *Legal protection of the individual's image against unauthorised commercial exploitation in South Africa: A critical evaluation of existing law and suggestions for law reform* [Doctoral dissertation, Stellenbosch University]. Stellenbosch University. Retrieved October 12, 2025, from https://scholar.sun.ac.za/handle/10019.1/128896

Violence Against Persons (Prohibition) Act, 2015 (Nigeria).

Waitangi Tribunal. (2011, July 2). *Ko Aotearoa Tēnei: Report on the Wai 262 claim released*. https://www.waitangitribunal.govt.nz/en/news/ko-aotearoa-tenei-report-on-the-wai-262-claim-released

Walter, M., & Carroll, S. R. (2020). Indigenous data sovereignty, governance and the link to Indigenous policy. In M. Walter, T. Kukutai, S. R. Carroll, & D. Rodriguez-Lonebear (Eds.), *Indigenous data sovereignty and policy* (pp. 1–20). Routledge. https://doi.org/10.4324/9780429273957

Walter, M., Lovett, R., Maher, B., Williamson, B., Prehn, J., Bodkin-Andrews, G., & Lee, V. (2021). Indigenous data sovereignty in the era of big data and open data. *Australian Journal of Social Issues, 56*(2), 143–156. https://doi.org/10.1002/ajs4.141

Wells v. Atoll Media (Pty) Ltd., [2010] 4 All SA 548 (WCC).

Weslow, D. E., Nuzum, S., & Rigizadeh, S. (2025, May 16). *Copyright Office issues key guidance on fair use in generative AI training*. Wiley Rein LLP. Retrieved July 28, 2026, from https://www.wiley.law/alert-Copyright-Office-Issues-Key-Guidance-on-Fair-Use-in-Generative-AI-Training

Westkamp, G. (2024, April 18). *Borrowed plumes: Taking artists' interests seriously in artificial intelligence regulation* [Working paper]. SSRN. Retrieved October 12, 2024, from https://doi.org/10.2139/ssrn.4799179 (papers.ssrn.com)

Wininger, A. (2023, November 29). *Beijing Internet Court recognizes copyright in AI-generated images*. China IP Law Update. Retrieved May 12, 2026, from https://www.chinaiplawupdate.com/2023/11/beijing-internet-court-recognizes-copyright-in-ai-generated-images/

World Intellectual Property Organization. (2001). *Intellectual property needs and expectations of traditional knowledge holders: WIPO report on fact-finding missions on intellectual property and traditional knowledge (1998–1999)*. https://www.wipo.int/publications/en/details.jsp?id=283

World Intellectual Property Organization. (2012). *The protection of traditional knowledge: Draft articles—Facilitators' text (WIPO/GRTKF/IC/21/REF/FACILITATORS TEXT)*. https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=203839

World Intellectual Property Organization. (2023). *Documentation of traditional knowledge and traditional cultural expressions* (Background Brief No. 9). https://www.wipo.int/publications/en/details.jsp?id=4695

World Intellectual Property Organization. (2024a). *Generative artificial intelligence (GenAI): The main concepts*. https://www.wipo.int/web-publications/patent-landscape-report-generative-artificial-intelligence-genai/en/1-generative-ai-the-main-concepts.html

World Intellectual Property Organization. (2024b). *WIPO Treaty on Intellectual Property, Genetic Resources, and Associated Traditional Knowledge*. Retrieved October 30, 2025, from https://www.wipo.int/wipolex/en/treaties/textdetails/19849

World Intellectual Property Organization. (2024). *The protection of traditional cultural expressions: Draft articles* (WIPO/GRTKF/IC/47/5). Retrieved July 18, 2026, from https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=642379

Wiredu, K. (1996). *Cultural universals and particulars: An African perspective*. Indiana University Press.

Young, J. O. (2008). *Cultural appropriation and the arts*. Blackwell Publishing.

Yu, W. F., et al. (2025). AI as a co-creator and a design material: Transforming the ideation and evaluation stages of the design process. *Design Studies*. Advance online publication. https://www.sciencedirect.com/science/article/pii/S0142694X25000158

Zacchini v. Scripps-Howard Broadcasting Co., 433 U.S. 562 (1977).

Zeleza, P. T. (2024, December 20). The rule of law in Africa: A reappraisal. *The Elephant*. Retrieved October 12, 2025, from https://www.theelephant.info/opinion/2024/12/20/the-rule-of-law-in-africa-a-reappraisal/

JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 6, Issue 1 (2026) p.263-297
https:doi.org/10.52907/jipit.2026.606

Constitutional Governance and Digital Identity Transformation in Kenya

*Stephen Larzen Juma**

ABSTRACT

Kenya's transition from Huduma Namba to Maisha Namba marks a significant shift in the architecture of digital governance. While successive administrations have promoted digital identity platforms as instruments of efficiency, transparency, and inclusion, evidence points to the contrary. The very systems designed to broaden access are generating new forms of exclusion, particularly for undocumented youth, rural and pastoral communities, and marginalized populations. This contradiction sits at the heart of the tension between Kenya's constitutional guarantees of equality, privacy, and meaningful public participation, and the lived experience of digital citizenship. The existing gap is that digital identity systems are treated more as a technical issue and less as a governance issue, including transparency, accountability, and equitable access to citizenship rights. This study argues that Kenya's digital identity reforms have prioritized administrative efficiency while inadequately addressing constitutional governance principles necessary for inclusive access to citizenship rights. The findings reveal that Kenya's digital identity platforms continue to enhance efficiency and reach of public service delivery, but have also intensified patterns of exclusion rooted in document poverty and infrastructure inequality. Judicial interventions have repeatedly exposed gaps in Data Protection Impact Assessments and weak enforcement of the constitutional safeguards contained in Article 31 on privacy and Article 27 on equality in the 2010 Constitution. The author assesses Kenya's experience alongside selected international digital identity systems, such as Estonia's rights-based e-identity

* Stephen Larzen Juma is a Kenyan public affairs professional and scholar specializing in international political economy, governance, peacebuilding, and social cohesion. He holds a Master of Public and International Affairs from the University of Pittsburgh and is a Fulbright FLTA alumnus. His work focuses on public policy, human rights, Pan- Africanism, and inclusive development.

model and Venezuela's politicized Carnet de la Patria system, to suggest digital identity governance reforms urgently needed in Kenya.

Keywords: Digital Identity, Data Rights, Participatory Governance, Exclusion, Surveillance.

TABLE OF CONTENTS

ABSTRACT 263

I. INTRODUCTION 265

II. DIGITAL IDENTITY AND GOVERNANCE: A MULTI-THEORETICAL APPROACH 267

III. DIGITAL IDENTITY GOVERNANCE IN KENYA 270

- *A. Historical Evolution of Digital Identity Governance in Kenya* 270
- *B. The Architecture of the Digital State and its Governance Objectives* 272
- *C. Power, Surveillance, Privacy, and Digital Governance in Kenya* 275
- *D. Implications of Digital Identity Exclusion and Poor Governance* 276
- *E. Key Challenges in Kenya's Digital Identity Ecosystem* .. 280

IV. COMPARATIVE STUDY OF DIGITAL IDENTITY SYSTEMS IN GLOBAL CONTEXT 282

- *A. Data Governance and Social Control: Lessons from Venezuela's Carnet de la Patria* *282*
- *B. Comparative Analysis of Kenya's Maisha Namba and Venezuela's Carnet de la Patria* *285*
- *C. Lessons from other Select Jurisdictions* *288*

V. POLICY RECOMMENDATIONS FOR KENYA 290

VI. CONCLUSION 294

REFERENCES 296

I. INTRODUCTION

Despite Kenya's constitutional commitment to equality and inclusion, significant demographics of its population remain excluded from identity systems. The 2024 FinAccess Household Survey reports that approximately 25.8 million Kenyan adults possess a national identity card, while about 2.3 million adults remain without one (KNBS et al., 2024). Young people aged 18-25 constitute 80.5% of adults without national identification, representing nearly 1.9 million individuals (KNBS et al., 2024). Identity exclusion also reflects broader socio-economic inequalities: rural exclusion stands at 12.6%, more than double the urban rate, and youth account for nearly half of the rural excluded population. These figures illustrate how identity exclusion intersects with existing patterns of marginalization and inequality.

The consequences of lacking legal identity extend beyond the absence of an identification document. Individuals without national identity cards face barriers to accessing banking services, registering SIM cards, securing formal employment, enrolling in educational institutions, voting, accessing healthcare, receiving humanitarian assistance, and benefiting from social protection programs (Human Rights Research, 2025). Such challenges are particularly significant for young people who are intended beneficiaries of government initiatives such as the Hustler Fund and the National Youth Opportunities Towards Advancement (NYOTA) program, both of which require valid national identification (Ministry of Micro, Small and Medium Enterprises Development, 2025). Consequently, identity-based exclusion may reinforce existing socio-economic inequalities rather than alleviate them.

A growing body of scholarship has examined Kenya's digital identity landscape, particularly in relation to *Huduma Namba* and its implications for privacy, data protection, exclusion, citizenship, and human rights (Hersey & Weitzberg, 2023; Privacy International & CIPIT, 2019). Studies have highlighted concerns regarding the potential exclusion of historically marginalized

groups, including the Nubian community, and have questioned how digital identity systems may reproduce existing inequalities through administrative and technological processes (Article 19, 2021; Mwangi & Bosire, 2021). Other scholars have explored the constitutional, legal, and governance implications of digital identity programs, especially in relation to participation, accountability, and state power (Hersey & Weitzberg, 2023).

While this literature provides important insights into the human rights and legal dimensions of digital identity, there remains scope for a more integrated examination of digital identity as a governance infrastructure that simultaneously shapes administrative efficiency, access to citizenship, service delivery, and exercise of rights. Existing studies often address these issues separately, focusing either on technological implementation, legal compliance, privacy concerns, or exclusion. This study therefore contributes to the literature by bringing these dimensions together within a governance framework that examines how digital identity systems operate as instruments of public administration, citizen-state relations, and democratic governance.

Accordingly, this study investigates how Kenya's digital identity system can be governed in ways that enhance administrative efficiency while safeguarding constitutional rights and promoting inclusive participation in the country's digital transformation. The study draws on Michel Foucault's concept of Biopower to examine how states classify and manage populations through administrative technologies; Alexander Galloway's theory of Protocol Governance to analyze how digital architectures and system rules shape access and control; and Engin Isin and Evelyn Ruppert's framework of Digital Citizenship to explore the relationship between digital technologies, rights, and belonging. To situate Kenya's experience within a broader global context, the study also undertakes a comparative analysis of Venezuela's Carnet de la Patria and considers lessons from Estonia's e-identity system and India's Aadhaar program. These cases provide both cautionary and best-practice perspectives on the governance

conditions that promote inclusion, accountability, and constitutional rights, or contribute to exclusion, surveillance, and social control.

This paper is organized into six chapters. Chapter One introduces the study by outlining the research problem, objectives, research questions, significance of the study, theoretical framework, and literature review. Chapter Two examines the conceptual and theoretical foundations of digital identity governance, drawing on the theories of Biopower, Protocol Governance, and Digital Citizenship. Chapter Three analyses Kenya's digital identity framework, focusing on the evolution of Huduma Namba and Maisha Namba, the legal and institutional framework, and key governance challenges relating to privacy, accountability, and inclusion. Chapter Four presents a comparative analysis of selected international digital identity systems, including Venezuela's Carnet de la Patria, Estonia's e-identity system, and India's Aadhaar program, to identify lessons for Kenya. Chapter Five synthesizes the findings and proposes policy and governance recommendations for developing a digital identity system that is efficient, rights-respecting, accountable, and inclusive. Chapter six is the conclusion.

II. DIGITAL IDENTITY AND GOVERNANCE: A MULTI-THEORETICAL APPROACH

This study adopts an integrated conceptual framework that combines Michel Foucault's concept of biopower, Alexander Galloway's theory of protocol governance, and Engin Isin and Evelyn Ruppert's framework of digital citizenship to explain how digital identity systems shape governance, citizenship, and access to rights. These theories demonstrate that digital identity systems are not just technical tools for identification but governance infrastructures that influence who is recognized by the state, who can access public services, and who can participate fully in social, economic, and political life.

First, Michel Foucault's concept of biopower explains how modern states exercise power by managing life rather than relying solely on coercion or force. Instead of simply governing territory, states govern populations through systems of registration, classification, surveillance, and regulation that make people 'visible' and therefore governable (Foucault, 1977). As Foucault argues, modern power works by 'making life and letting die', shifting attention from punishment to the administration of life itself. Through institutions such as censuses, health systems, and digital identity programs, governments acquire the capacity to monitor populations, allocate resources, and regulate access to rights, services, and opportunities. This perspective helps explain why digital identity systems are simultaneously instruments of service delivery and mechanisms of governance. In the context of digital identity systems, registration and data collection enable the state to identify citizens, monitor service delivery, and allocate resources. However, biopower also highlights how those who are not registered may become administratively invisible and consequently excluded from essential services. The theory helps explain how digital identity systems can simultaneously facilitate inclusion and reproduce exclusion.

Secondly, Alexander Galloway's theory of *protocol governance* argues that, in digital societies, power is exercised not only through laws or centralized authority but also through the technical rules and standards embedded within digital networks. These 'protocols' govern how people access information, services, and digital platforms, often in ways that appear neutral but carry significant political and governance implications (Galloway, 2004). Galloway (2004) contends that 'protocol is how control exists after decentralization', meaning that control is increasingly exercised through the architecture of digital systems rather than direct coercion. In digital identity systems, authentication requirements, interoperability standards, and verification processes become governance mechanisms that determine who can participate, access services, and exercise digital citizenship.

In Kenya's digital identity ecosystem context, the authentication requirements, biometric verification processes, data-sharing arrangements, and eligibility conditions embedded within platforms such as eCitizen, SHA, and iTax shape who can access services and under what conditions. These technical protocols can unintentionally create barriers for individuals lacking documentation, connectivity, or digital literacy, thereby institutionalizing exclusion through system design.

Finally, Isin and Ruppert's framework of *digital citizenship* argues that citizenship is increasingly enacted through digital technologies and data infrastructures rather than solely through traditional legal or political institutions. They contend that citizens perform acts of citizenship by interacting with digital platforms to access public services, exercise rights, communicate with government, and participate in civic life (Isin & Ruppert, 2015). As they observe, 'to be digital is to become a citizen through data', highlighting how digital recognition increasingly shapes belonging and entitlement. Their framework shows that digital identity systems do more than verify identity; they redefine who can claim rights, participate in governance, and access state services. Consequently, exclusion from digital identity systems can undermine both citizenship and equal participation in democratic life.

Taken together, Foucault's concept of *biopower*, Galloway's theory of *protocol governance*, and Isin and Ruppert's framework of *digital citizenship* provide a comprehensive lens for understanding Kenya's digital identity reforms. Foucault explains how digital identity enables the state to classify, monitor, and govern populations through data. Galloway demonstrates that governance is increasingly embedded in the technical architecture of digital systems, where protocols determine who can access services and under what conditions. Isin and Ruppert show that citizenship is now increasingly exercised through digital platforms, making digital recognition a prerequisite for claiming rights and participating in public life. Collectively, these theories

support the study's argument that digital identity systems are governance infrastructures whose legitimacy depends not only on administrative efficiency but also on constitutional principles of inclusion, accountability, transparency, privacy, and meaningful citizen participation.

These theoretical lenses map out how the collection of citizen data acts as a gatekeeper to basic rights, and how the style of governance dictates whether a digital shift empowers a country's citizens or alienates them. The following section provides a detailed breakdown of this framework in relation to data rights and participatory governance in Kenya.

III. DIGITAL IDENTITY GOVERNANCE IN KENYA

A. Historical Evolution of Digital Identity Governance in Kenya

A fundamental shift occurred in the early 2000s when the Government of Kenya embraced information and communication technology as a catalyst for public sector reform. The e-Government Strategy of 2004 and the National ICT Policy of 2006 laid the foundation for digital governance by promoting interoperability, electronic service delivery, and integrated government information systems. These reforms culminated in the National Digital Master Plan 2022–2032, which positions digital identity as the cornerstone of Kenya's digital economy and an essential enabler of efficient public administration, economic transformation, and the achievement of the Sustainable Development Goals (Ministry of ICT, 2022).

The enactment of the Data Protection Act (2019) (DPA) marked a significant milestone in Kenya's digital governance framework. The Act established comprehensive legal standards governing the collection, processing, storage, and sharing of personal data while creating the Office of the Data Protection Commissioner (ODPC) to oversee compliance (ODPC, 2020). More importantly, it affirmed that digital transformation must oper-

ate within a constitutional framework that safeguards privacy, accountability, transparency, and citizens' rights.

These principles were tested during the implementation of the National Integrated Identity Management System (NIIMS), commonly known as *Huduma Namba*. Introduced in 2019 to consolidate fragmented government databases into a single biometric identity system, NIIMS promised to improve service delivery and eliminate duplication. However, in *Katiba Institute & Another v Attorney General & Others [2020] eKLR*, the High Court held that the government's implementation failed to satisfy constitutional requirements by proceeding without an adequate Data Protection Impact Assessment (DPIA) and sufficient legal safeguards to protect personal data. The Court reaffirmed that administrative efficiency cannot override the constitutional rights to privacy, equality, and public participation (Privacy International, 2021).

The government subsequently introduced *Maisha Namba* in 2023 as the successor to *Huduma Namba*, presenting it as a more secure and legally compliant digital identity framework capable of integrating key public platforms, including eCitizen, the Social Health Authority (SHA), and the Kenya Revenue Authority (KRA) (Hubz Media, 2025). Nevertheless, civil society organizations and human rights advocates continued to raise concerns regarding data sharing, surveillance, exclusion of undocumented and marginalized populations, and the adequacy of public participation. These concerns prompted renewed legal challenges and further judicial scrutiny, with courts emphasizing the necessity of completing Data Protection Impact Assessments and ensuring meaningful citizen participation before full implementation.

This historical trajectory reveals that Kenya's identity systems have evolved from instruments of colonial population control into sophisticated digital governance infrastructures. While technologies have changed, the central governance question lingers on: How can the state make its population administratively visible without undermining the constitutional rights of

the very citizens it seeks to govern? The recurring legal disputes surrounding both *Huduma Namba and Maisha Namba suggest that Kenya's digital identity reforms have consistently prioritized administrative efficiency while struggling to fully institutionalize the constitutional principles of inclusivity, transparency, accountability, privacy, and public participation. Bridging this governance gap constitutes the central concern of this paper.*

B. The Architecture of the Digital State and its Governance Objectives

Kenya has one of Africa's most advanced digital governance ecosystems. For example, the eCitizen portal allows users to access more than 9,000 government services and hosts roughly 32 million accounts (Citizen Digital, 2024). The Kenya Revenue Authority's iTax platform, linked to national ID numbers, has over 6 million registered entities (KRA, 2023). The Social Health Authority (SHA), which has replaced the National Health Insurance Fund (NHIF), also has one digital platform that registers and tracks all health insurance claims, and has approximately 24 million registered members (TNX Africa, 2025). The National Transport and Safety Authority runs the Transport Integrated Management System (TIMS), which links driver licensing to national identity databases. In the education sector, the Kenya Education Management Information System (KEMIS) and the National Education Management Information System (NEMIS) centralize learner and institutional data across the country, while the Independent Electoral and Boundaries Commission (IEBC) operates biometric voter registration related to national identity systems.

These platforms reflect a shared vision of moving from a siloed, paper-based public administration to one that is integrated and data-driven; one in which people's access to rights, services, and civic participation is conditioned on their ability to verify themselves to the state through a digital identity. The ambition is well-founded, but it also concentrates power in ways that de-

serve scrutiny. When identity verification becomes the gateway to healthcare, education, financial services, and democratic participation, the stakes of registration become existential. Understanding who is part of these systems and who is not is therefore one of the most pressing governance questions.

Kenya's digital identity system serves a dual purpose: it functions as a technical platform for delivering public services and as an instrument of governance. The government's digital identity agenda is designed to improve administrative efficiency, reduce fraud, enhance interoperability, and strengthen service delivery through a lifelong Unique Personal Identifier (UPI) assigned to every citizen (Gichobi, 2026). By integrating identity across government institutions, the system seeks to eliminate duplicate records, improve targeting of public resources, and provide citizens with seamless access to state services. From a governance perspective, these objectives represent a significant step toward modernizing public administration.

However, the findings indicate that the pursuit of administrative efficiency has created tensions with constitutional principles of inclusion, equality, and accountability. Foucault's (1977) concept of *biopower* provides an important lens for understanding this contradiction. Foucault (1977) argues that modern states govern by classifying, registering, and monitoring populations through administrative systems. Digital identity therefore makes citizens visible to the state and enables more effective planning and service delivery. At the same time, individuals who remain outside the registration system become administratively invisible and are often excluded from the rights and benefits attached to legal recognition. In Kenya, the absence of a digital identity can restrict access to healthcare, social protection, financial services, and civic participation, illustrating how systems intended to promote efficiency can also become mechanisms of exclusion.

This tension is reflected in the constitutional challenges surrounding digital identity implementation. Although the Constitution of Kenya (2010) guarantees the rights to privacy, equal-

ity, non-discrimination, and public participation under Articles 31, 27, and 10, respectively, they have not been fully realized in Kenya's digital identity governance system. For example, in the *Katiba Institute & Another v Attorney General & Others* case, the High Court held that the *Huduma Namba* rollout failed to meet these constitutional standards. The *Huduma Namba* rollout was unconstitutional because it proceeded without a prior DPIA and without sufficient safeguards to protect the right to privacy (Privacy International, 2022).

The judge stated that large-scale identity processing must comply with the DPA, 2019, and Article 31 of the Constitution, since administrative efficiency cannot justify exposing citizens to unjustified surveillance or the misuse of personal data. The judgment therefore set a precedent that digital identity systems must pursue efficiency without compromising constitutional rights.

This theoretical insight is further supported by Galloway's work on protocol governance. Galloway (2004) notes that 'the digital language of control is made of codes indicating where access to some information should be allowed or denied. We're no longer dealing with a duality of mass and individual' from the modern era. Instead, individuals become 'dividuals,' and masses become samples, data, markets, or 'banks' (Galloway, 2004, p. 39). He explains that power in digital systems is embedded in the rules and procedures that regulate access rather than in legislation alone. In Kenya, requirements such as prior possession of a birth certificate or national identity document determine who can enroll in *Maisha Namba*. Civil society organizations argue that these conditions disproportionately disadvantage individuals who already lack foundational documents, particularly those from marginalized communities (Namati Kenya, 2025). Consequently, technical protocols become governance mechanisms that unintentionally reproduce *document poverty*.

The analysis also aligns with Isin and Ruppert's (2015) concept of *digital citizenship*, which argues that citizenship is increasingly exercised through digital platforms. As access to gov-

ernment services becomes dependent on digital identity, legal recognition within these systems increasingly determines who can claim rights and participate fully in public life. Kenya's digital identity system is thus not merely a technological innovation but a governance infrastructure that shapes citizenship and access to rights. To achieve its intended objectives, constitutional safeguards, inclusive design, and accountability mechanisms must be embedded in both the legal framework and the system's technical architecture. Building on these theoretical foundations, the following section examines the relationship between power, surveillance, privacy, and digital governance

C. Power, Surveillance, Privacy, and Digital Governance in Kenya

Michel Foucault's (1977) concept of biopower provides an important explanation for these developments. According to Foucault (1977), modern states increasingly govern by collecting information, classifying populations, and making citizens continuously visible through administrative systems. Digital identity, biometric registration, and AI-enabled surveillance expand the state's ability to monitor individuals and regulate access to public services (Foucault, 1977). While this visibility can improve policy planning, enhance security, and facilitate service delivery, it also concentrates significant power within state institutions and creates opportunities for excessive monitoring and control.

This concern is directly relevant to the central argument of this study, which examines how digital identity systems reshape the relationship between citizens and the state. Rather than functioning solely as neutral administrative tools, digital identity infrastructures can become instruments through which state power is exercised, particularly when linked to surveillance technologies and automated decision-making systems. As Bradshaw and Howard (2018) observe, digital platforms can facilitate the collection and strategic use of data in ways that influence behavior and reinforce political authority. Consequently, the governance of digital identity raises not only questions of efficiency

and inclusion but also broader constitutional concerns regarding privacy, accountability, and the protection of fundamental rights.

The suspension of the NTSA Instant Fines Traffic Management System by the High Court following constitutional petitions illustrates these tensions in practice, highlighting the risks of allowing automated systems to make decisions affecting citizens' rights without adequate procedural safeguards (Correspondent, 2026). The case demonstrates that while digital technologies can improve governance, they must operate within constitutional limits that guarantee transparency, accountability, and due process. Digital governance should therefore complement rather than replace human judgment and constitutional protections, ensuring that technological innovation serves citizens without undermining democratic oversight or civil liberties.

Having examined the theoretical and constitutional dimensions of digital identity governance, the following section considers the practical implications of digital identity exclusion and poor governance in Kenya.

D. Implications of Digital Identity Exclusion and Poor Governance

1. Case Study I: Data Governance and Control in Kenya.

To provide empirical context for the discussion, Table 1 presents registered user data across Kenya's key digital identity and governance platforms against the country's projected 2025 population of 53.3 million.

Platform / System	Country	Registered Users	Description / Function	Source
Kenyan Population	Kenya	53.3 million	Total projected population, 2025	KNBS, 2025
Kenyan ID holders	Kenya	25.8 million	Total population with IDs 2025	KNBS, 2025

Platform / System	Country	Registered Users	Description / Function	Source
Huduma Namba	Kenya	18 million	National Integrated Identity Management System (NIIMS); legacy biometric registry	Kenya News Agency, 2025
Maisha Namba	Kenya	13 million	Unique Personal Identifier system replacing Huduma Namba; active rollout	Fintech News Kenya, 2024
eCitizen Platform	Kenya	32 million accounts	Central digital portal for 9,000+ government services	ICT Authority Kenya, 2025
SHA (Social Health Authority)	Kenya	23.3 million	Unified digital health insurance and registration system	TNX Africa, 2025
iTax (KRA)	Kenya	6.1 million	Online tax filing and compliance system	KRA, 2023
KEMIS / NEMIS	Kenya	12.6 million learners	National education management and student data system	Capital FM Kenya, 2025

The data presented in Table 1 demonstrate that Kenya has made significant progress in building an integrated digital governance ecosystem, reflecting the state's commitment to improving administrative efficiency, strengthening service delivery, and modernizing public administration. Specifically, the eCitizen platform has registered 32 million accounts and provides access to more than 9,000 government services (ICT Authority Kenya, 2025). The Social Health Authority (SHA) has enrolled 23.3 million individuals, KEMIS/NEMIS manages records for 12.6 million learners, iTax serves over 6.1 million taxpayers, while the ongoing rollout of Maisha Namba has registered approximately 13 million people (Fintech News Kenya, 2024). Together, these

systems illustrate the increasing integration of Kenya's digital governance architecture around a common identity infrastructure.

This development demonstrates how digital identity has become the foundation upon which access to public services is increasingly organized. The growing interoperability between government platforms means that identity systems are no longer isolated administrative tools; rather, they function as gateways through which citizens interact with multiple state institutions. The adoption of the Unique Personal Identifier (UPI) under *Maisha Namba* further reflects the state's ambition to establish a single, trusted identity that enables seamless engagement with government services throughout an individual's life. From this perspective, digital identity is fulfilling its intended objective of creating a more coordinated and efficient public sector.

However, the findings also show that the success of digital transformation cannot be evaluated solely through platform expansion or registration figures. Equally important is whether all citizens can access the identity infrastructure on which these systems depend. Despite the growth of digital government, approximately 2.3 million adults in Kenya still lack national identity cards, with young people aged 18–25 accounting for 80.5% of this undocumented population (KNBS et al., 2024). This finding is significant because exclusion from legal identity increasingly translates into exclusion from the broader digital governance ecosystem. As government services become more interconnected, individuals without foundational identity documents face barriers to accessing healthcare, education, social protection, financial services, and other public programs. The benefits of digital governance therefore remain unevenly distributed, reinforcing the study's argument that inclusion within identity systems is a prerequisite for meaningful participation in an increasingly digital state.

Beyond these concerns about inclusion, this study finds that the implications of exclusionary and weakly accountable digital

governance extend to the state's fiscal capacity and broader development objectives. Although Kenya has invested significantly in digital platforms, the expected benefits remain constrained by persistent gaps in compliance and participation. According to the Kenya Revenue Authority (KRA), 6.3 million taxpayers filed income tax returns for the 2022 year of income, representing a 14.5% increase from the previous year but only a fraction of the more than 22 million registered Personal Identification Number (PIN) holders (KRA, 2023). Similarly, during the financial year ending June 2025, only 156,232 of the 618,201 registered companies, approximately 25.2%, remitted corporate income tax, leaving nearly three-quarters of registered firms outside the tax net (KRA, 2025). These figures indicate that digitalization alone does not automatically generate higher compliance or stronger public finance outcomes. While digital identity systems can improve the state's ability to identify taxpayers and coordinate administrative data, their effectiveness ultimately depends on citizens' willingness and ability to participate in the formal system.

This finding reiterates that the value of digital identity extends beyond administrative efficiency; sustainable digital governance requires legitimacy, inclusion, and public trust. Foucault's (1977) concept of biopower helps explain this relationship by illustrating how administrative systems increase the state's capacity to classify, monitor, and manage populations. Digital identity enhances the visibility of citizens within state systems and facilitates access to public services and government programs. However, where individuals remain outside foundational identity systems, they risk exclusion from the benefits increasingly delivered through digital platforms. The challenge, therefore, is not simply to expand registration but to ensure that digital governance strengthens rather than undermines constitutional principles of equality, participation, and inclusion.

Similarly, Galloway's (2004) theory of protocol governance suggests that technical systems are most effective when the rules embedded within them are perceived as legitimate, fair,

and accessible. Digital platforms may improve administrative coordination, but they are less effective in promoting compliance when citizens face barriers to participation or lack confidence in public institutions. This explains why the expansion of digital infrastructure does not necessarily produce corresponding improvements in tax compliance or state revenue mobilization.

The findings therefore reinforce the central argument of this study that Kenya's digital identity reforms have largely prioritized administrative efficiency while paying comparatively less attention to the constitutional governance foundations required for inclusive and effective implementation. A narrow and unreliable tax base is not merely a fiscal challenge but also a governance challenge, reflecting broader issues of inclusion, legitimacy, and citizen-state relations. Consistent with the values enshrined in Articles 10 and 201 of the Constitution of Kenya (2010), sustainable digital governance requires transparency, accountability, public participation, equitable access, and trust. Strengthening these constitutional foundations is essential if digital identity systems are to support not only efficient administration but also fiscal legitimacy, inclusive citizenship, and long-term national development.

Having established the governance context and its implications, the following section identifies the key challenges facing Kenya's digital identity ecosystem

E. Key Challenges in Kenya's Digital Identity Ecosystem

The first challenge is structural exclusion through documentation requirements. This persistent challenge arises from strict dependency on foundational documents such as birth certificates, parental identity cards, or prior registration records. Such requirements create a cycle of 'document poverty' in which individuals cannot enter digital governance systems, including Maisha Namba, eCitizen, or SHA. For example, undocumented youth in Kibra or Moyale may be unable to access national identity registration, thereby foreclosing access to HELB funding,

SHA services, and voter registration. This pattern of exclusion directly contradicts Articles 27 and 38 of the Constitution.

A second challenge is weak enforcement of data protection and privacy rights. Although Kenya's DPA, 2019 provides a strong legislative framework, enforcement remains inconsistent. Major biometric systems, including *Huduma Namba* and *Maisha Namba*, have faced judicial scrutiny for insufficient DPIAs, as established in *Katiba Institute v Attorney General* (2021). This enforcement gap exposes citizens to risks of surveillance, unauthorized data sharing, and profiling, particularly as platforms increasingly integrate across SHA, iTax, and eCitizen.

A third challenge is the digital divide and unequal access to participation. Kenya's digital governance assumes universal digital access in a context where disparities in internet connectivity, digital literacy, and infrastructure remain significant. Rural counties and informal settlements face barriers to accessing online platforms, excluding large populations from SHA registration, tax compliance, and public participation forums. While eCitizen records over 30 million accounts, a substantial proportion of rural citizens remain underrepresented, limiting their ability to engage meaningfully in governance.

A fourth challenge is limited transparency and public participation in digital governance design. Most decisions about digital identity system design and deployment are centralized within state agencies, principally the Ministry of Interior and the National Registration Bureau, with limited meaningful public consultation. This undermines Article 10 of the Constitution, which requires public participation, transparency, and inclusivity in governance processes. It also reduces public trust and fuels resistance to reforms such as *Maisha Namba* that courts have repeatedly had to adjudicate.

To contextualize Kenya's experience within broader global trends, the following section presents a comparative study of digital identity systems in selected jurisdictions.

IV. COMPARATIVE STUDY OF DIGITAL IDENTITY SYSTEMS IN GLOBAL CONTEXT

A. Data Governance and Social Control: Lessons from Venezuela's Carnet de la Patria

Venezuela's Carnet de la Patria ('Homeland Card') offers an important comparative case for understanding how digital identity systems can evolve when governance is driven by political interests rather than constitutional safeguards. Introduced in 2016 through the state-operated Sistema Patria, the card was initially presented as a mechanism to improve the delivery of social welfare and public services (Human Rights Watch, 2018). Over time, however, it became closely associated with political surveillance, monitoring of citizens, and the distribution of state benefits in ways that raised serious human rights concerns.

Evidence indicates that access to government welfare programs, including food assistance distributed through the Local Committees for Supply and Production (CLAP), became closely linked to registration under the *Carnet de la Patria*. Human rights organizations reported that individuals perceived to support the political opposition, or those who had not registered on the platform, were less likely to receive food aid and other social benefits (Human Rights Watch, 2018). Consequently, a system introduced to improve administrative efficiency gradually became a mechanism through which access to essential public services could be influenced by political considerations rather than universal citizenship rights.

The Venezuelan experience illustrates that the greatest risk does not lie in digital identity technology itself, but in the governance arrangements surrounding it. The *Carnet de la Patria* consolidates biometric information, socio-economic data, and welfare records within a highly centralized state-controlled platform with limited transparency, weak independent oversight, and inadequate data protection safeguards (Freedom House, 2021). In such an environment, the concentration of personal

data created opportunities for surveillance, political profiling, and discriminatory allocation of public resources. Legal identity ceased to function as a neutral administrative tool and instead became an instrument through which the state could influence citizens' behavior and political participation.

This experience is well explained through Foucault's (1977) concept of *biopower*, which argues that modern states exercise power by classifying, monitoring, and managing populations. In Venezuela, digital identity extended beyond identifying citizens to regulating access to food, healthcare, and other essential services. State power is therefore exercised not through direct coercion alone, but through administrative systems that determine who qualifies for public support. Galloway's (2004) theory of *protocol governance* further explains how this control is embedded within the technical architecture of the platform itself. The rules governing registration, verification, and eligibility appear administrative, yet they effectively determined who could access state benefits. Governance is therefore exercised through digital protocols that structure participation and access.

The Venezuelan case is presented not as a prediction of Kenya's future, but as a cautionary example of the governance risks associated with centralized digital identity systems that lack effective constitutional safeguards. Kenya operates within a markedly different institutional context, supported by the Constitution of Kenya, 2010, the DPA, 2019, an independent judiciary, and an active civil society capable of scrutinizing government action. These institutions provide important safeguards against arbitrary use of digital identity systems. Nevertheless, the strength of a digital identity system lies not only in the sophistication of its technology but also in the governance principles that regulate its design, implementation, and use.

Platform / System	Country	Registered Users	Description / Function	Source
Population	Venezuela	30,254,079	Total national population	World Bank DataBank, 2023
Carnet de la Patria	Venezuela	16.6 million	State digital ID tied to access to food subsidies, welfare, and social services	Reuters, 2018; Human Rights Watch, 2018

The data presented in the table above illustrate the central role that Carnet de la Patria plays within Venezuela's system of public administration. With approximately 16.6 million users registered for the Carnet de la Patria in a country of about 30.3 million people, the platform reaches more than half of the national population, making it one of the country's most significant governance infrastructures (World Bank DataBank, 2023). Its broad coverage demonstrates the capacity of digital identity systems to support large-scale coordination of public services and welfare programs.

However, the Venezuelan experience also demonstrates that widespread adoption alone is not an indicator of good governance. Unlike conventional digital identity systems designed primarily for identification and service delivery, the *Carnet de la Patria* became closely linked to the distribution of food subsidies, social welfare, and other essential public benefits. Human rights organizations have documented concerns that access to these programs was, in some instances, influenced by political considerations, raising questions about equality, transparency, and the protection of citizens' rights (Human Rights Watch, 2018).

The lesson for Kenya is clear: expanding digital identity coverage should be accompanied by strong constitutional safeguards, transparency, accountability, and independent oversight to ensure that digital identity remains a tool for inclusion rather than social or political control.

B. Comparative Analysis of Kenya's Maisha Namba and Venezuela's Carnet de la Patria

A comparison between Kenya's *Maisha Namba* and Venezuela's *Carnet de la Patria* demonstrates that digital identity systems are not inherently inclusive or exclusionary; rather, their governance outcomes depend on the legal, political, and institutional environments within which they operate. Both systems seek to improve administrative efficiency by creating a unique digital identity through which citizens access government services. However, they differ fundamentally in their governance objectives, implementation approaches, and implications for constitutional rights.

Kenya presents Maisha Namba as a public sector modernization initiative designed to improve identity management, eliminate duplication, enhance interoperability across government agencies, and facilitate efficient service delivery (Gichobi, 2026). Recent reports indicate that the system has contributed to reducing processing backlogs for identity cards, passports, and birth registration, reflecting the potential benefits of integrated digital governance (Fintech News Kenya, 2024). In contrast, Venezuela's Carnet de la Patria was introduced primarily as a mechanism for administering welfare programs through the Sistema Patria. While it similarly links citizens to public services and subsidies, human rights organizations have documented concerns regarding its use in monitoring beneficiaries and influencing access to social assistance (Freedom House, 2024). This comparison highlights that the long-term impact of digital identity systems depends not only on their technical design but also on the legal, institutional, and constitutional safeguards governing their operation. The same technologies that improve service delivery can produce very different outcomes depending on the extent of transparency, accountability, independent oversight, and protection of fundamental rights.

From the perspective of Foucault's (1977) concept of biopower, both systems demonstrate how digital identity enables the

state to classify, monitor, and manage populations. Registration makes citizens visible within administrative systems and facilitates the allocation of public resources. However, Foucault also reminds us that visibility creates opportunities for control. In Kenya, this power is principally exercised to coordinate service delivery across platforms such as eCitizen, SHA, and iTax. In Venezuela, evidence suggests that the same administrative capacity has been extended to monitor political behavior and regulate access to welfare benefits, illustrating how identical technologies may produce very different governance outcomes depending on the surrounding political institutions (Human Rights Watch, 2021).

Galloway's (2004) theory of protocol governance further explains these differences by demonstrating that governance is embedded in the technical rules governing digital systems. In Kenya, debate has largely centered on whether the protocols underpinning *Maisha Namba* comply with constitutional requirements relating to data protection, privacy, transparency, and public participation. The High Court's decision in *Katiba Institute & Another v Attorney General & Others* [2021] eKLR established that digital identity systems must satisfy constitutional safeguards, including meaningful public participation and adequate data protection measures, before implementation. Venezuela presents a different governance challenge. There, digital protocols reportedly determine eligibility for subsidies and welfare programs in ways that have been criticized for discriminating on political grounds rather than applying neutral administrative criteria (Freedom House, 2024). The comparison demonstrates that technical architecture is never politically neutral; the rules embedded within digital systems ultimately determine how power is exercised.

The comparison is equally instructive through the lens of digital citizenship. Isin and Ruppert (2015) argue that citizenship is increasingly enacted through digital infrastructures that mediate access to rights and public participation. In Kenya, dig-

ital citizenship is evolving through the integration of public services under *Maisha Namba*, raising legitimate concerns about the exclusion of undocumented populations from healthcare, education, financial services, and social protection. Nevertheless, the constitutional framework provides avenues for judicial review, civil society engagement, and legal accountability, as demonstrated by litigation surrounding *Huduma Namba*. In Venezuela, however, digital identity has been widely criticized for transforming access to welfare into a politically contingent privilege, thereby weakening the neutrality of citizenship and eroding equal access to state services (Human Rights Watch, 2021).

The comparison therefore reinforces the central argument of this study that the governance of digital identity is equally as important as the technology itself. Kenya's digital identity ecosystem demonstrates that substantial gains in administrative efficiency are achievable through integrated digital governance. However, efficiency alone cannot be a measure of success. The Constitution of Kenya (2010) requires public participation, transparency, accountability, equality, access to information, and respect for privacy as foundational principles of governance. These constitutional values distinguish a democratic digital identity system from one that becomes an instrument of surveillance or exclusion. The Venezuelan experience illustrates the risks that emerge when digital identity is implemented without adequate institutional safeguards, independent oversight, and rights-based governance. For Kenya, the lesson is to ensure that technological innovation remains firmly anchored in constitutionalism. Only by balancing efficiency with inclusion, accountability, transparency, and citizen participation can *Maisha Namba* realize its intended objective of strengthening both public administration and democratic citizenship. In addition to the Venezuelan case study, lessons from other select jurisdictions provide further insight into the governance of digital identity systems

C. Lessons from other Select Jurisdictions

Kenya's digital identity reforms should be understood within the broader global movement toward digital governance, where states increasingly rely on digital identity systems to improve service delivery, strengthen public administration, and expand access to government services. Internationally, legal identity is recognized as a critical foundation for inclusive development. The World Bank's Identification for Development (ID4D) initiative identifies trusted and inclusive digital identity systems as essential for improving access to public services, financial inclusion, and economic participation (World Bank, 2018). Similarly, Sustainable Development Goal (SDG) 16.9 calls upon states to provide legal identity for all by 2030 as a means of promoting inclusive and accountable governance (United Nations, 2015). Kenya's *Maisha Namba* program is situated within these global aspirations. However, comparative experience demonstrates that the success of digital identity systems depends not only on administrative efficiency but also on the extent to which they are designed and implemented in a manner consistent with constitutional principles and protections.

India's Aadhaar program offers an important lesson for Kenya because it illustrates both the benefits and risks associated with large-scale biometric identity systems. Introduced in 2009 by the Unique Identification Authority of India (UIDAI), Aadhaar has become the world's largest biometric identity program, linking residents' identities to fingerprint, iris, and demographic data (UIDAI, 2023). The program is particularly relevant to Kenya because, like *Maisha Namba*, it seeks to create a reliable and unified identity infrastructure capable of improving public service delivery and reducing duplication within government systems. While Aadhaar has enhanced identity verification and administrative efficiency, studies have documented instances where biometric authentication failures prevented legitimate beneficiaries, particularly elderly persons, manual laborers, and rural populations, from accessing essential services (World Bank, 2018). The

significance of the Indian experience lies not merely in these exclusionary outcomes but in the legal response that followed. In Justice K.S. Puttaswamy (Retd.) v Union of India (2018), the Supreme Court of India upheld the program's legitimacy while emphasizing that digital identity initiatives must remain subject to constitutional scrutiny, particularly with respect to privacy, necessity, and proportionality (UIDAI, 2023). For Kenya, the case demonstrates that even where a digital identity system serves legitimate governmental objectives, constitutional compliance must remain central to its design and implementation. The Indian experience therefore highlights the need for legal safeguards capable of preventing exclusion while ensuring that technological innovation does not undermine fundamental rights.

Estonia provides a contrasting but equally valuable lesson by demonstrating how digital identity systems can be developed within a framework of transparency, accountability, and citizen control. Through its X-Road platform, Estonia facilitates secure data sharing among public institutions without requiring all personal information to be stored in a single centralized database (e-Estonia, 2022). More importantly, citizens are able to monitor access to their personal information through auditable access logs, thereby promoting transparency and strengthening public trust in governmental data practices. The relevance of the Estonian model to Kenya lies in its demonstration that digital identity systems can enhance administrative efficiency while simultaneously reinforcing constitutional values. Rather than treating efficiency and rights protection as competing objectives, Estonia integrates technological innovation with governance mechanisms that promote accountability, transparency, and individual control over personal data. These features provide useful lessons for Kenya as it seeks to operationalize the constitutional principles of openness, accountability, and data protection within its evolving digital identity framework.

The experiences of India and Estonia demonstrate that the principal challenge in digital identity governance is not simply

establishing a technologically effective identification system but ensuring that such systems operate within a framework that protects constitutional rights and promotes inclusive access to public services. India illustrates the risks of exclusion and the importance of judicially enforceable constitutional safeguards, while Estonia demonstrates how transparency and accountability mechanisms can strengthen public trust and legitimacy. These comparative lessons are directly relevant to Kenya's *Maisha Namba* program because they underscore the need for digital identity reforms to be evaluated not only in terms of administrative performance but also in terms of their impact on inclusion, privacy, accountability, and access to rights. Together, the two jurisdictions provide a useful framework through which Kenya's ongoing digital identity reforms can be assessed and improved. Drawing on the findings and comparative analysis presented above, this section sets out policy recommendations for strengthening Kenya's digital identity governance framework

V. POLICY RECOMMENDATIONS FOR KENYA

The findings of this study demonstrate that Kenya's digital identity reforms have been characterized by tensions between administrative efficiency and constitutional governance. The analysis reveal persistent concerns regarding compliance with constitutional and statutory safeguards, exclusion of vulnerable populations from identity registration systems, inadequate public participation, and barriers to meaningful access arising from digital inequalities. The recommendations below are therefore directed specifically at addressing these identified shortcomings.

i) Strengthen compliance with constitutional and data protection safeguards

The implementation of digital identity systems should be anchored in strict compliance with constitutional and statutory requirements governing privacy, data protection, and admin-

istrative accountability. A recurring theme in this study is the tendency to prioritize technological deployment before fully satisfying procedural safeguards intended to protect fundamental rights.

In Nubian Rights Forum & 2 Others v Attorney General & 6 Others [2020] eKLR, the High Court held that the rollout of the National Integrated Identity Management System (NIIMS) could not proceed without an adequate regulatory framework and a DPIA. Similarly, in Katiba Institute & Another v Attorney General & Another [2024] eKLR, the High Court emphasized the necessity of complying with data protection requirements in the implementation of the *Maisha Namba* program. These decisions demonstrate that DPIAs are not merely technical exercises, but constitutional safeguards intended to identify and mitigate risks to privacy and other fundamental rights.

Accordingly, all future digital identity initiatives should be subjected to comprehensive and publicly available DPIAs before implementation. In addition, the ODPC should be strengthened through enhanced oversight powers and adequate institutional resources to ensure effective monitoring of compliance with the DPA, 2019.

ii) Reduce exclusion through more accessible registration frameworks

This study established that exclusion remains one of the most significant challenges facing Kenya's digital identity ecosystem. Large numbers of citizens, particularly undocumented youth, residents of border regions, pastoralist communities, and other marginalized groups, continue to experience difficulties in accessing identity documents that are necessary for participation in social, economic, and political life.

To address this challenge, the government should expand registration services in underserved areas through sustained mobile registration programs and targeted outreach initiatives.

Particular attention should be directed toward communities historically affected by documentation barriers. Registration procedures should also provide reasonable and transparent alternative mechanisms for establishing identity where conventional documentary requirements are unavailable.

This recommendation is consistent with Articles 10, 27, and 56 of the Constitution, which require inclusivity, equality, and protection of marginalized groups, as well as the World Bank's ID4D principles advocating universal and accessible legal identity systems (World Bank, 2018).

iii) Institutionalize meaningful public participation and transparency

A major finding of this study is that digital identity reforms in Kenya have frequently generated controversy because affected communities perceive them as being introduced without sufficient consultation, transparency, or public engagement. Yet public participation is a constitutional requirement under Articles 10 and 232 of the Constitution and is particularly important where governmental programs involve the collection and processing of sensitive personal information.

The government should therefore institutionalize public participation throughout the design, implementation, and review of digital identity systems. This process should extend beyond formal consultations and include accessible public information campaigns, publication of policy documents and impact assessments, and structured engagement with civil society organizations, data protection experts, and affected communities.

Meaningful participation would not only fulfill constitutional obligations but would also improve public trust, legitimacy, and acceptance of digital identity reforms.

iv) Address digital inequalities that hinder access to identity-related services

The study further established that the increasing digitization of government services creates a risk that existing social and economic inequalities will be reproduced within digital governance systems. Limited internet access, inadequate digital literacy, unreliable electricity infrastructure, and unequal access to digital devices continue to affect many rural and marginalized communities.

Kenya should therefore treat digital inclusion as an essential component of digital identity governance. This requires continued investment in connectivity infrastructure, digital literacy programs, and community-based digital access centers, particularly in underserved regions. Importantly, digital identity systems should not entirely replace alternative service-delivery channels. Maintaining accessible non-digital options is necessary to ensure that citizens are not denied access to public services solely because of technological barriers.

v) Establish a rights-based framework for oversight, accountability, and redress

The effectiveness of digital identity systems ultimately depends on the existence of mechanisms capable of protecting individuals from exclusion, administrative error, and violations of fundamental rights. The study demonstrated that citizens who encounter difficulties within digital identity systems often face limited avenues for remedy and accountability.

Kenya should therefore strengthen rights-based oversight mechanisms by establishing accessible grievance and appeals procedures for persons affected by registration errors, exclusion, or misuse of personal data. Oversight institutions, including the ODPC and relevant constitutional commissions, should play a more active role in monitoring the human rights implications of digital identity programs.

Such safeguards would operationalize the constitutional values of accountability, human dignity, equality, and access to justice while ensuring that digital identity systems function as instruments of inclusion rather than exclusion.

VI. CONCLUSION

The findings reveal that Kenya has made significant progress in digitizing government services and improving administrative efficiency. Digital platforms have enhanced coordination across institutions, reduced duplication, and expanded the accessibility of certain public services. However, the study also found that these gains have not been experienced equally across the population. Persistent documentation barriers, digital inequalities, and challenges affecting marginalized and vulnerable groups continue to limit the ability of many individuals to participate fully in the country's digital governance framework. As a result, the promise of inclusion that underpins digital transformation remains only partially realized.

The study further established that constitutional compliance remains a critical challenge in the implementation of digital identity programs. Judicial interventions concerning NIIMS/Huduma Namba and, more recently, *Maisha Namba* demonstrate that the pursuit of efficiency cannot override constitutional and statutory safeguards relating to privacy, data protection, public participation, and administrative accountability. These decisions underscore the broader finding that the legitimacy and sustainability of digital identity systems depend not only on technological functionality but also on adherence to constitutional principles and the rule of law.

Comparative analysis of selected jurisdictions reinforced this conclusion. The experiences of India and Estonia demonstrated that successful digital identity systems require more than technological innovation; they require effective legal safe-

guards, transparent governance structures, and mechanisms that promote public trust while reducing the risk of exclusion. These lessons highlight the importance of ensuring that Kenya's digital transformation agenda remains firmly anchored in constitutional values.

This study is subject to certain limitations. It relied primarily on doctrinal and qualitative analysis of legal frameworks, policy documents, judicial decisions, and secondary literature. Consequently, it did not undertake empirical field research involving affected communities, government agencies, or system users. Future research may therefore benefit from empirical studies examining the lived experiences of citizens interacting with digital identity systems, particularly among marginalized populations, as well as assessments of the long-term impacts of *Maisha Namba* and other digital governance initiatives on access to public services and the exercise of citizenship rights.

Ultimately, the study concludes that the success of Kenya's digital identity reforms should not be measured solely by technological advancement, administrative convenience, or enrollment figures. Rather, their success will depend on whether they promote inclusive access to services, uphold constitutional rights, foster public trust, and ensure that no citizen is excluded from full participation in the digital state. Only by balancing efficiency with constitutional governance can Kenya realize the transformative potential of digital identity systems while safeguarding democratic citizenship and equal access to rights.

REFERENCES

Article 19. (2021, October 21). *Kenya: Digital identification systems must protect human rights*. Article 19 Eastern Africa. https://www.article19.org/resources/consortium-calls-for-reforms-implementation-of-kenyas-digital-id/

Bradshaw, S., & Howard, P. N. (2018). *Challenging truth and trust: A global inventory of organized Bradshaw, S., & Howard, P. N. (2018). Challenging truth and trust: A global inventory of organized social media manipulation (Working Paper No. 2018.1). Computational Propaganda Research Project, Oxford University. https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2018/07/ct2018.pdf*

Central Bank of Kenya, Kenya National Bureau of Statistics, & Financial Sector Deepening Kenya. (2024). *2024 FinAccess household survey report*. https://www.centralbank.go.ke/wp-content/uploads/2024/12/2024-FINACCESS-HOUSEHOLD-SURVEY-MAIN-REPORT.pdf

Constitution of Kenya. (2010).

Correspondent, G. A. | K. (2026, April 7). *Kenya Dispatch: High Court suspends automated traffic fines system, testing due process rights*. *Jurist*.

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

e-Estonia. (2022). *e-Identity: Secure digital identity and digital society*. https://e-estonia.com/solutions/estonian-e-identity/id-card/

Eggers, D. (2014). *The Circle*. Alfred A. Knopf.

Fintech News Kenya. (2024). *Kenya's Maisha Namba rollout gathers pace as digital identity reforms continue*.

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (A. Sheridan, Trans.). Pantheon Books. (Original work published 1975)

Freedom House. (2021). *Freedom on the Net 2021: Venezuela*. https://freedomhouse.org/country/venezuela/freedom-net/2021

Galloway, A. R. (2004). *Protocol: How control exists after decentralization*. MIT Press.

Gichobi, K. (2026, February 20). *Digital government transformation in Kenya: From manual* Government of Kenya.

GSMA. (2021). *Digital identity in Rwanda: Case study on inclusive digital transformation*. https://researchictafrica.net/research/digital-identity-in-rwanda-case-study-conducted-as-part-of-a-ten-country-exploration-of-socio-digital-id-systems-in-parts-of-africa/

Hersey, L., & Weitzberg, K. (2023). Digital ID, statelessness, and exclusion in Kenya: The case of the Nubians. *Journal of Eastern African Studies*, 17(1-2), 181–201. https://doi.org/10.1080/17531055.2023.2201948

Hubz Media. (2025, October 12). *Maisha Namba: Kenya's next-generation digital ID*.

Human Rights Watch. (2018, May 18). *Hostages of hunger: Venezuela's food crisis*

and the Carnet Human Rights Watch. (2021a). *Automated repression: Digital surveillance and human rights*.

Human Rights Watch. (n.d.). Defending human rights worldwide. Retrieved August 15, 2026, from https://www.hrw.org/

Katiba Institute & Another v Attorney General & 2 Others [2021] eKLR. http://kenyalaw.org

Kenya National Bureau of Statistics. (2025). *Kenya population and housing survey report*. Kenya Revenue Authority. (2023). *Kenyan ruling on Huduma Namba*. https://privacyinternational.org

Ministry of Micro, Small and Medium Enterprises Development. (2025). *NYOTA call for* Namati Kenya. (2025). *Expert witness submissions on exclusion risks in the Maisha Namba regime*. Ndungu, T. (2024, November 28). *30M users, 22,515 services: President Ruto hails E-citizen as a game-changer in governance. Citizen Digital*. https://citizen.digital/article/30m-users-22515-services-president-ruto-hails-e-citizen-as-a-game-changer-in-governance-n353698

OECD. (2021). *Digital government and Estonia's e-governance model*. https://www.oecd.org

Office of the Data Protection Commissioner. (2020). *Data Protection Act, 2019:* Office of the Data Protection Commissioner. (2025). *Guidance on biometric data Office of the Data Protection Commissioner. (n.d.). Home page. Retrieved August 31, 2026, from https://www.odpc.go.ke/*Isin, E. F., & Ruppert, E. (2015). *Being digital citizens*. Rowman & Littlefield International.

PIN registration. Retrieved August 17, 2026, from https://www.kra.go.ke/business/companies-partnerships/companies-partnerships-pin-taxes/companies-partnerships-pin-registration

Privacy International, & Centre for Intellectual Property and Information Technology Law. (2019). *Identity and exclusion in Kenya: Biometrics and the Huduma Namba* (Research Report). Privacy International. https://privacyinternational.org/news-analysis/3350/why-huduma-namba-ruling-matters-future-digital-id-and-not-just-kenya

Privacy International. (2022). *Data protection impact assessments and ID systems: The 2021 processing and DPIA compliance in Kenya.*

TNX Africa. (2025). *Over 23 million Kenyans registered in Social Health Authority*.

UIDAI. (2023). *About Aadhaar*. Government of India. https://uidai.gov.in/en/my-aadhaar/about-your-aadhaar.html

United Nations. (2015). *Transforming our world: The 2030 Agenda for Sustainable Development*. https://sdgs.un.org/2030agenda

World Bank. (2018). *ID4D: Identification for Development global dataset and principles*. https://id4d.worldbank.org

World Bank. (2023). *Digital ID systems for inclusive development*. https://id4d.worldbank.org/guide

JIPIT

Journal of Intellectual Property and Information Technology Law (JIPIT)
ISSN: 2788-6727 – Volume 6, Issue 1 (2026) p.299-338
https:doi.org/10.52907/jipit.2026.610

Data Rights and Participatory Governance: An Analysis of Health Data Governance in Kenya

Silvia W. Mwangi & Maria N. Bosita***

ABSTRACT

As many countries, including Kenya, increasingly leverage technology and data to improve health systems and deliver better healthcare outcomes, models of health data governance continue to attract growing global attention. Effective data governance is essential for promoting the safe, equitable, and responsible use of health information, particularly as digital health systems expand. This has increased the need to ensure that individuals are meaningfully involved in decisions concerning the collection, use, and sharing of their health data because it directly affects their rights, privacy, and trust in the health system. Owing to the broad nature of health data governance, this paper focuses specifically on participatory governance as a means of enhancing public trust, transparency, and accountability in Kenya's health sector. The authors investigate the existing legal framework regulating the health sector with a focus on the Constitution and the Digital Health Act (No. 15 of 2023) to assess whether they adequately facilitate meaningful public participation in decisions concerning the governance and secondary use of health data. This paper hypothesizes that although Kenya has established a comprehensive legal framework for health data governance, the framework does not sufficiently provide for effective participatory governance in the management of health data. Drawing on the experience of the United Kingdom, this paper evaluates how different mechanisms may contribute to greater public trust, accountability, and transparency. It argues that sustainable health data governance requires more than technical safeguards; as Kenya continues to expand digital health systems, health data governance must

* Advocate of the High Court of Kenya, LL. B Hons, PGDL (Kenya School of Law), Legal Researcher, National Council for law Reporting (Kenya Law). The author has a passion for legal research, data analytics, and policy. Email: sylviahwanjira01@gmail.com

** Advocate of the High Court of Kenya, LL. B Hons, PGDL (Kenya School of Law), Data Protection Officer, Certified (PECB), Regulatory Compliance Associate, Romer Services Limited. The author's interest is in the intersection of law and technology, with a strong interest in data protection and digital governance.

be matched by a commitment to meaningful and continuous public participation. The authors conclude by making recommendations for strengthening participatory governance within Kenya's existing legal and institutional framework, including the adoption of health data stewardship mechanisms informed by data trust principles.

Keywords: Data Ownership, Data Trusts, Data Stewardship, Health Data Governance, Participatory Governance

TABLE OF CONTENTS

ABSTRACT 299
I. INTRODUCTION 301
II. HEALTH DATA AND PARTICIPATORY DATA GOVERNANCE 304
III. LEGISLATIVE FRAMEWORK 309
A. *Constitutional Framework* 310
B. *Supporting Statutory and Policy Framework* 311
C. *Digital Health Act, (No. 15 Of 2023)* 314
IV. PARTICIPATORY DATA GOVERNANCE IN THE UNITED KINGDOM 315
A. *Data Trusts as a Model for Data Governance in the UK Healthcare Sector* 316
B. *Governance Structure and Operation of Data Trusts* 318
C. *Implementation of Data Trusts in the UK* 319
V. AN ANALYSIS OF PUBLIC TRUST AND PARTICIPATORY GOVERNANCE IN KENYA'S HEALTHCARE SYSTEM 323
VI. THE WAY FORWARD FOR KENYA'S HEALTH DATA GOVERNANCE 328
A. *Embed Public Trust as a Guiding Principle of Health Data Governance* 328
B. *Amend the DHA to Establish a Health Data Advisory Council* 329
C. *Develop a Kenyan Model of Data Stewardship Informed by the Concept of Data Trusts* 330
D. *Institutionalize Continuous Public Participation in Health Data Governance* 331
VII. CONCLUSION 332
REFERENCES 334

I. INTRODUCTION

On 19 October 2023, Kenya saw a major shift in the governance and regulation of its health sector. The President assented to four statutes that now frame the country's move toward a more integrated health system: specifically, the Social Health Insurance Act, 2023, the Digital Health Act, 2023, the Primary Health Care Act, 2023, and the Facilities Improvement Financing Act, 2023. This paper focuses on the Digital Health Act, 2023 (hereafter 'DHA'), which introduces a structured approach to health data governance. The substratum of the DHA reflects a wider policy view that treats health data as a strategic national asset rather than a by-product of clinical or administrative processes. Section 3 of the DHA also provides for the safe sharing and transfer of personally identifiable health data between health facilities both within Kenya and outside the jurisdiction, as well as guidelines for the development of standards for the provision of telemedicine, e-learning, and m-Health.

These reforms align with national development goals under the Bottom-Up Economic Transformation Agenda (BETA) and Vision 2030, both of which prioritize universal access to quality healthcare (Ireri et al., 2025). The enactment of the laws on digital health in Kenya was also introduced to address some of the longstanding challenges in the health information system, including a lack of health equipment, insufficient supply of medicine, and foul play between medical insurers and hospital facilities, among others, which resulted from a lack of system interoperability (Walubengo, 2023).

To address these challenges, section 15 of the DHA establishes an Integrated Health Information System intended to anchor a nationwide health data ecosystem. Importantly, the enactment of the DHA did not mark the beginning of Kenya's digital health journey. Some of the innovations observed previously include the use of Electronic Medical Records (EMRs) that improve patient record keeping, reduce clerical errors, and ensure availability of

continuous care for patients (Doctors Explain Digital Health Co., LTD., 2025). More recently, the Digital Health Agency has spearheaded the rollout of Taifa Care Health Management Information System (HMIS) as an integrated platform supporting clinical management, laboratory services, pharmacy management, and health financing processes, while the establishment of the Kenya National Public Health Institute and its National Public Health Intelligence Information System (NPHIIS) reflects the growing use of digital technologies in disease surveillance, outbreak preparedness, and public health intelligence (Ng'ang'a-Kna, 2026). Further, the electronic Community Health Information System (eCHIS) has strengthened data collection and referral management by enabling community health promoters to capture and transmit health information electronically (Li et al., 2022).

The adoption of digital healthcare has also enabled data-driven decision-making, particularly through the implementation of District Health Information Software 2 (DHIS2) across almost all public health facilities (Oware et al., 2025). The DHIS2 is an open-source platform that supports the real-time collection, visualization, and reporting of health data utilized by county governments as well as the national government to allocate resources, proactively respond to outbreaks, and monitor disease trends, facilitating public health campaigns (Oware et al., 2025). Additionally, a health database this large with integrated datasets offers enormous value for research as it can reveal population-level trends, improve disease surveillance, support clinical innovation, and strengthen evidence-based policy (Transform Health, 2024). Governance must therefore balance multiple interests: the rights of individuals whose data is used, the responsibilities of institutions that steward the data, and the public value that may arise from research, innovation, and service improvement (Kariotis et al., 2020).

While these reforms demonstrate how digital systems can strengthen efficiency, equity, and planning within the health sector, they also introduce new forms of risk if not carefully imple-

mented. The increased digitization and centralization of health information under the Centralized Integrated Health Information System (CIHIS) risks exposing individuals to data breaches, unauthorized access, and misuse of sensitive health information (OECD, 2015). These risks are particularly significant given the highly sensitive nature of health data and the potential consequences of its misuse (OECD, 2015). Limited public participation can create a gap between formal compliance with data-protection requirements and the legitimacy of data-governance practices for the affected individuals (Field et al., 2024). This is particularly important where health data is increasingly reused for research, policy development, and disease surveillance (Aymé et al., 2026). Individuals may bear the privacy and social risks associated with these uses while having little influence over the purposes for which their data are subsequently used or the safeguards governing such use. The resulting imbalance can weaken public trust and undermine the willingness of individuals to participate fully in digital health systems. To this end, there is a growing interest in governance models that emphasize collective oversight and public participation, such as data trusts, data cooperatives, and health information commons (Hummel et al., 2020). These models aim to build and sustain what is often described as a 'social license', reflecting the idea that public acceptance of data use extends beyond formal legal compliance and depends on trust, legitimacy, and perceived fairness (Hummel et al., 2020).

Against this backdrop, this paper examines whether the legal framework governing Kenya's health sector enables meaningful public participation in the governance of health data. This question is rooted in the Constitution of Kenya, 2010, which identifies public participation as a foundational national value under Article 10 and recognizes both the right to privacy under Article 31 and the right to the highest attainable standard of health under Article 43. These rights intersect directly in the context of digital health, where personal data is both a critical resource for public welfare and a potential site of vulnerability

(Tiffin et al., 2019). As Kenya deepens its investment in digital health infrastructure, the legitimacy and sustainability of these systems will increasingly depend on whether affected communities have a meaningful voice in how their data is collected, used, shared, and protected.

This paper assesses whether the country's evolving legal framework is capable of supporting a participatory, trustworthy, and rights-respecting digital health ecosystem. Accordingly, this paper is further divided into six parts. Part II delves into the contextual rights on health data governance, data rights, and participatory governance. Part III analyzes the legislative framework relating to health data governance in Kenya in order to assess the extent to which it facilitates meaningful public participation in decisions concerning health data. Part IV provides a comparative analysis with the current framework in the UK to provide insights for Kenya. Part V addresses public trust and participatory governance within Kenya's healthcare system. Part VI presents the way forward for Kenya by suggesting key recommendations to strengthen participatory governance. Finally, Part VII concludes the paper.

II. HEALTH DATA AND PARTICIPATORY DATA GOVERNANCE

Data, as defined under section 2 of the DHA, refers broadly to any information that is processed or recorded, in most cases in electronic form. The section further defines health data as a subset of data concerning the health status of a natural person or health services, including records of past, present, or future physical or mental health and any information generated during health care delivery. The section also defines the term 'Data Governance' as 'the overall management of the availability, usability, integrity, and security of data used in an organization'. While these definitions capture the operational aspects of data management, health data governance extends beyond technical administration. It encompasses institutional, legal, and organi-

zational frameworks that regulate how health data is collected, accessed, shared, and stored while ensuring individual rights are protected (Transform Health, 2022). Data governance therefore provides a broader framework within which decisions concerning access and interoperability are made.

Large-scale health data underpins modern medical research and is central to improving health systems for the public good. When patient datasets are collected and analyzed at scale, they support evidence-based medicine by allowing clinicians and researchers to move beyond isolated cases and rely on trends drawn from real-world practice (OECD, 2022). Aggregated datasets make it possible to identify what works, for whom, and under what conditions, leading to more effective and safer clinical decisions (Hassan, 2025). Richer and more diverse health datasets also enable the development of precision therapies. By analyzing variations in patient histories, genetics, treatment responses, and outcomes, researchers can tailor interventions to specific populations or even individual patients (Hassan, 2025). In this way, health data not only drives scientific innovation but also ensures that new treatments and models of care are grounded in actual patient experience and deliver tangible benefits for the public good (Hassan, 2025). However, these benefits can only be made possible where appropriate legal and governance frameworks are in place to ensure that health data collected is used in a manner that protects individual rights and promotes public trust (WHO, 2021).

Similarly, precision medicine relies on integrating diverse data sources, including clinical records, genetic tests, and patient-reported outcomes, among others, to tailor interventions. Structured health data combined with other information form *'a valuable treasure trove'* that can improve medical knowledge and patient outcomes (OECD, 2022). Beyond individual care, health data is vital for public health surveillance and planning. Integrated health information systems such as the CIHIS established under the DHA can monitor disease trends, assess service needs,

and guide policy (Bernadette et al., 2018). When supported by reliable governance mechanisms, integrated health systems can enhance scientific innovation and more effective health service delivery, thus promoting sustainable healthcare.

However, despite the clear benefits of an integrated health system, in particular with regard to data sharing, the scale, sensitivity, and nature of health data present significant challenges. Health data includes highly sensitive personally identifiable information; due to its sensitivity it is an attractive target for malicious actors, making strong legal, technical, and organizational safeguards necessary to prevent unauthorized access and data breaches. These risks become even more pronounced where multiple public and private entities exchange data through interoperable digital platforms, which in turn undermines public trust and discourages participation in digital health initiatives (Musoni et al., 2026). These governance challenges are not merely hypothetical. They have already begun to emerge within Kenya's digital health transformation agenda as seen in *Okoiti v Prime Cabinet Secretary and Cabinet for Foreign and Diaspora Affairs & 3 others (Petition E816 of 2025) [2025] KEHC 18939 (KLR) (Constitutional and Human Rights) (19 December 2025) (Ruling)*, which touches on the Cooperative Framework 'the Framework' between the Government of Kenya and the government of the United States of America on Health.

The Framework seeks to support the implementation of an extensively integrated digital health ecosystem. Under paragraph 2.5 of the Framework, the parties propose the integration of Taifa Care Health Management Information System (HMIS), the Electronic Community Health Information System (eCHIS), the National Public Health Intelligence Information System (NPHI-IS), the All-Disease Outbreak Module (ADAM), the National Logistics Management Information System (NLMIS), Social Health Authority digital platforms, Health Information Exchange infrastructure, national and county health data banks, and a National Health Cloud into a unified health information architecture.

The petitioner in the case argues that the Framework ought to have undergone parliamentary approval and meaningful public participation before implementation. The petitioner further contends that the Framework poses significant data privacy and protection concerns because medical information constitutes sensitive personal data protected under Article 31 of the Constitution of Kenya and the Data Protection Act (Cap 411). According to the petitioner, the contemplated collection, integration, and potential sharing of health data through interconnected national systems could affect individual privacy rights where adequate safeguards, transparency measures, and public oversight mechanisms are lacking. The petitioner further alleges that the Framework undermines the constitutional principle of public participation. Although the interim orders that initially halted aspects of the implementation process and proposed data transfers were subsequently lifted, the issues raised in the proceedings underscore the legal and governance challenges that accompany the development of integrated digital health systems.

These proceedings illustrate that effective health data governance requires not only technical safeguards and compliance with data protection laws, but also transparent decision-making, institutional accountability, and meaningful public participation in decisions concerning the collection, use, and sharing of health data.

Notably, the question of who 'owns' health data has led to innovative governance models (Piasecki & Cheah, 2022). Instead of exclusive private or public ownership, hybrid stewardship arrangements such as data trusts are emerging. According to the Global Partnership on Artificial Intelligence (GPAI) Data Governance Working Group (2021), data trusts are legal structures where a trusted steward manages data on behalf of a community under agreed rules. They involve appointing fiduciaries charged with protecting donors' interests. In practice, such models embed the principles of transparency and shared decision-making that are designed to govern the use of beneficiaries' data in a

rights-preserving way. At a theoretical level, scholars recommend focusing less on simplistic ownership and more on governed access as well as responsible stewardship (Aurora, 2019). These emerging models provide a useful comparative benchmark for assessing whether Kenya's health data governance framework adequately balances the rights of data subjects and the public value of health data.

While debates concerning ownership focus on institutional control over health data, modern health data policies emphasize the rights of individuals over their personal data. These include rights to be informed about data use, to grant or withdraw consent, to access and correct one's records, and to privacy (OECD, 2022). For instance, section 61 of the DHA in Kenya explicitly upholds patient privacy and calls for compliance with data protection principles, reflecting the requirement to respect individuals' rights (CIPESA, 2024). Legislation such as the EU General Data Protection Regulation (GDPR) similarly demonstrates that data rights, including access, consent, and anonymity among others, should be legally codified. In practice, this means giving patients control tools such as consent choices and portability and setting strict limits on data sharing to protect confidentiality (Transform Health, 2024). However, legal rights alone are insufficient to ensure effective health data governance. Effective implementation calls for the incorporation of participatory governance models that allow affected persons to collectively engage in decisions about how health data is collected, used, and shared, thereby strengthening accountability, public trust, and the legitimacy of digital health systems.

Therefore, participatory governance seeks to ensure involvement of data beneficiaries in stewardship, build accountability, and foster public confidence. In the health data context, participation can take the form of patient advocacy groups in setting research priorities or reviewing data-sharing proposals (FNIH, 2025). The goal is to ensure that data use reflects social values and that individuals see direct benefits. This has been recog-

nized in international policy instruments such as the OECD's Health Data Governance Recommendation (2022) and Transform Health's Principles for Digital Health Governance (2024), which urge the implementation of national health data governance frameworks that incorporate key principles such as accountability, interoperability, security, and respect for individual rights, and promote cross-border cooperation in data sharing.

Implementing these principles requires more than isolated legal protections; it demands an integrated governance framework that aligns legal, institutional, and technical safeguards. In practice, this calls for the integration of previously fragmented data systems, including public health registries, electronic health records, and biobanks within a coherent legal and technical architecture. Comparative and proposed model laws similarly emphasize the need for an integrated governance approach grounded in shared standards on data rights, privacy, and consent. Such harmonization is essential to provide individuals and communities with stronger protections, clearer expectations, and a predictable legal environment for the use of health data. Drawing on this contextual perspective, the next section seeks to examine Kenya's legal framework in greater detail to assess whether it delivers an integrated model of health data governance that enables health research and innovation as well as safeguards individual rights and public trust.

III. LEGISLATIVE FRAMEWORK

The digitalization of the health sector in Kenya is grounded in a constitutional and statutory framework that seeks to balance access to healthcare, protection of personal data, and public participation. While several laws provide supporting safeguards relating to privacy, research, healthcare administration, and access to information, the Constitution of Kenya, 2010 and the DHA, 2023 occupy a central position in the present discussion because they frame the relationship between digital health gov-

ernance, individual rights, and public participation. Examining these laws together demonstrates the importance of legal coherence in health data governance and highlights the need for institutional arrangements that ensure digital transformation occurs in a manner that remains accountable to the public.

A. Constitutional Framework

The Constitution primarily guides the development of all other statutory laws and guarantees the right to the highest attainable standard of health while simultaneously safeguarding privacy, access to information, and participatory governance. Article 43(1)(a) of the Constitution guarantees every person the right to the highest attainable standard of health, including access to healthcare services and reproductive health care. This right provides the normative basis for the adoption of digital health technologies aimed at improving accessibility, efficiency, and quality of healthcare services.

The pursuit of improved healthcare cannot be detached from the constitutional protection of privacy. Article 31 guarantees every person the right not to have information relating to their private affairs unnecessarily revealed. This provision is directly engaged in the context of electronic health records, such as patient diagnoses, history of treatment, and biometric health information. Integrated health information systems and health research databases also involve collection, processing, storage, and, in some instances, sharing of sensitive personal health information, therefore increasing the risk of unauthorized access, disclosure, misuse, or surveillance. Article 31 therefore provides a constitutional safeguard requiring that health data is handled carefully, securely, and confidentially while ensuring the adoption of digital health technologies does not undermine individuals' right to privacy.

The Constitution also recognizes that legitimate governance requires more than simply protecting individual rights. Article

35, buttressed by the *Access to Information Act (Cap. 7M)*, gives effect to and supports transparency in the management of public health information; subject to lawful limitations outlined in section 6 of the Access to Information Act, which are aimed at protecting privacy and confidentiality. Article 10 further anchors public participation, transparency, and accountability as national values that bind all state organs, public officers, and entities whenever they enact, apply, or interpret law or implement public policy.

Articles 110 and 118 reinforce participatory legislative processes, requiring meaningful public involvement in law-making that affects the health sector and the governance of health data. Taken together, these provisions establish a constitutional mandate for a health data governance framework that advances access to healthcare while respecting privacy and enabling public participation in decisions affecting the use and management of health data.

The constitutional significance of participatory governance became particularly evident in *Okoiti v Prime Cabinet Secretary and 4 others (2025)*, challenging the Kenya and United States Cooperative Framework on Health. The petition was premised on the argument that health data governance is not merely a technical matter but one that implicates constitutional values relating to privacy, public participation, accountability, and oversight. As discussed in the second part of the paper above, the petition demonstrates that the constitutional principles of participation and privacy are increasingly being tested by emerging forms of digital health governance.

B. Supporting Statutory and Policy Framework

Several statutes and policy instruments complement the constitutional framework by regulating specific aspects of health data governance. The Health Act (Cap. 241) provides the foundational statutory framework for Kenya's health system and ex-

pressly recognizes the role of digital technologies in healthcare delivery. Section 105 establishes a Health Information System to facilitate the collection, management, and dissemination of health information. Sections 8 and 11 of the Act prohibit the disclosure of a patient's health information without their consent, subject to limited statutory exceptions, and place a strong emphasis on confidentiality, privacy, and data security. In doing so, it seeks to ensure that the adoption of digital health solutions contributes to improved health outcomes without undermining individual rights.

Similarly, the National e-Health Policy articulates Kenya's long-term vision for the integration of information and communication technologies within the health sector with the aim of achieving the highest standard of health through adoption and use of ICT (Ministry of Health, 2016). Chapter 4 of the policy promotes the use of interoperable digital health systems and underscores the need for secure storage, encryption, and controlled access to health data. The chapter also emphasizes compliance with data protection standards and supports the widespread adoption of electronic health (e-health) records. Its emphasis, however, remains largely technical, focusing on infrastructure, standards, and capacity building rather than participatory governance.

The Data Protection Act (Cap 411C) (DPA) 2019 provides the overarching legal framework for the processing of personal data in Kenya and is central to health data governance. Part V of the Act classifies health data as sensitive personal data, subjecting it to enhanced safeguards. Section 26 empowers individuals with enforceable rights, including the right to access, correct, and, in certain circumstances, delete their personal data. The above provisions of the DPA play a vital role in shaping the governance of electronic health records, digital health systems, and digital health infrastructure containing personal data. Nevertheless, it primarily adopts an individual rights-based approach and offers limited mechanisms for collective participation in decisions re-

garding the governance of large-scale health data ecosystems.

The Science, Technology and Innovation Act (Cap. 511) establishes institutional mechanisms intended to guide and coordinate research activities in Kenya, including research that relies on large-scale data resources such as health and biomedical data. The Act under Part III empowers the National Commission for Science, Technology and Innovation to establish the Advisory Research Committees as expert bodies that support the Commission in implementing national research priorities. From a health data governance perspective, these provisions demonstrate Kenya's reliance on expert-led advisory structures in shaping research policy and oversight. However, while the Act provides coordination, expertise, and reporting, it does not expressly require public or community participation in research, even where research activities involve sensitive health or biomedical data. As a result, decisions relating to use and governance of such data are largely left to the institutional and technical actors, raising concerns about limited participatory governance and insufficient representation of the affected individuals.

The Social Health Insurance Act (No. 16 of 2023) under section 3 outlines the objective of the Act, which is the establishment of public health insurance schemes with the aim of facilitating equitable access to healthcare services. Section 47 of the Act provides for the digitization of insurance processes with the aim of enhancing effectiveness and accountability, requiring that the same be done in line with the applicable data protection laws to safeguard patient data. While the Act promotes efficacy in healthcare administration, it provides limited governance of the large volume of sensitive health data collected or generated through these systems, particularly regarding data sharing, secondary use, and patient participation in decision-making. This brings out the governance issue of the expanding digitized and centralized health data systems without corresponding accountability and participatory mechanisms.

C. Digital Health Act, (No. 15 Of 2023)

The DHA under section 3 outlines the objective of the Act, which is to provide a dedicated legal framework for the provision of digital health services in Kenya. A central feature of the Act is the establishment of the Digital Health Agency under section 5, which is mandated to develop, operationalize, and maintain CI-HIS, as well as to facilitate the creation of shareable and portable personal health records in accordance with recognized standards and best practices. The Agency is also responsible for developing secure infrastructure for the exchange of health information and ensuring that health data are managed in a manner that supports continuity of care and informed decision-making.

The Act has been operationalized through subsidiary legislation, including the Digital Health (Data Exchange Component) Regulations, 2025 and the Digital Health (Health Information Management Procedures) Regulations, 2025. Collectively, these instruments provide detailed rules on interoperability, data exchange, health data sharing, health data banks, and patient access to health records. They also support the integration of existing digital health systems through shared infrastructure. In the same vein, the Digital Health Agency Strategic Plan 2025-2028 prioritizes the expansion of interoperable digital health systems and the National Digital Health Superhighway, reflecting the government's broader objective of building a data-driven and integrated healthcare ecosystem. Together, the Act and its subsidiary legislation demonstrate a deliberate effort to create an integrated and interoperable digital health ecosystem capable of supporting healthcare delivery and evidence-based decision-making.

Notwithstanding its detailed institutional and technical architecture, the DHA adopts a largely top-down governance model. While it recognizes consent as a prerequisite for access to identifiable health data, it does not provide for meaningful involvement of individuals in broader decisions affecting the governance, secondary use, or cross-border sharing of their health

data. Further, while the framework is extensive in regulating how health data is collected, stored, exchanged, and protected, it provides comparatively limited mechanisms for public participation in decisions concerning the governance of that data. The Act primarily conceives individuals as data subjects whose information requires protection through consent, access rights, and complaint mechanisms. It does not expressly provide for patient representation, citizen advisory structures, public deliberation processes, or participatory oversight mechanisms through which affected communities can influence decisions relating to secondary uses of health data, large-scale data integration, or health data-sharing arrangements, as raised in the *Okoiti v Prime Cabinet & 4 others* case. Consequently, the DHA provides a technical framework for health data governance but leaves unresolved the extent to which citizens should participate in shaping the governance and future use of their health data.

In conclusion, these constitutional provisions and the other legal instruments establish a legal foundation for health sector digitalization and interoperability in Kenya. However, they also create an inadequate governance framework characterized by institution-driven decision-making and implementation of technical safeguards as opposed to participatory governance. The above analysis demonstrates that the existing framework inadequately integrates participatory governance that would sufficiently enable public involvement in decisions concerning the collection, use, and sharing of health data. The next part of this paper seeks to conduct a comparative analysis with the UK to derive lessons that Kenya can implement to ensure that the health governance framework adequately addresses public participation.

IV. PARTICIPATORY DATA GOVERNANCE IN THE UNITED KINGDOM

The UK offers a useful comparative jurisdiction for Kenya because it has established a comprehensive legal and insti-

tutional framework governing the collection, sharing, and secondary use of health data through the National Health Service (NHS), while also confronting significant challenges relating to public trust, transparency, and participatory governance. The UK's experience demonstrates that effective health data governance depends not only on compliance with legal and technical requirements but also on maintaining public confidence through meaningful public participation and accountable governance structures. Although the institutional and healthcare systems of Kenya and the UK differ considerably, the governance challenges associated with balancing health data innovation, individual rights, and public trust are common to both jurisdictions. The UK experience therefore provides valuable comparative insights for assessing the strengths and limitations of Kenya's emerging health data governance framework and for identifying governance mechanisms capable of strengthening participatory decision-making.

A. Data Trusts as a Model for Data Governance in the UK Healthcare Sector

According to Souvatzi et al. (2024), trust is used to refer to the relationship where one has a reasonable belief in the ability of another person to do good or to deliver on their expressed commitment to do a certain action. It is widely acknowledged that trust plays a crucial role in the acceptability of data sharing practices, especially in healthcare (Kerasidou & Kerasidou, 2023). Individuals are more likely to support the collection, sharing, and secondary use of their health data where they believe that public institutions will use such information lawfully, transparently, and in the public interest (McKee et al., 2025). This is crucial, especially in the digital age where health technologies are increasingly being implemented (Unver & Odusola-Stevenson, 2025). The digitization of the NHS began in 2002, with the aim of becoming paperless by 2018 and achieving a core level of digitization by 2024. A major part of this plan involved the in-

troduction of Electronic Health Records (EHRs). The move from paper files to digital, highly mobile data created a new technological infrastructure that supported the digitization of health information (Baniulyte et al., 2023).

Notably, the NHS is the largest holder of health data, which creates favorable conditions for the establishment and promotion of a data-driven healthcare sector (Kerasidou & Kerasidou, 2023). The NHS is widely regarded as a public institution that holds and warrants public trust, where its main function is to provide support for the citizens' health and well-being. In the NHS Constitution for England (2012), the NHS is said to belong to the people; hence, it forms the basis of a trust relationship between the British public and itself. In this relationship, the public has the duty of funding the health service through the provision of taxes and use of its resources prudently, while the State has the responsibility of oversight and deliverance of appropriate care at the point of need (NHS Constitution for England, 2012).

Additionally, the UK has developed extensive policies and governance frameworks on health data sharing, participatory governance, and even artificial intelligence, which provide useful lessons for comparative analysis in this paper. It is important to note that, in recent years, data-sharing initiatives implemented through programs such as *care.data* and the General Practice Data for Planning and Research (GPDPR) program attracted significant public concern, particularly regarding transparency, the involvement of commercial actors, and the potential use of patient data beyond the purposes originally understood by the public (Macdonald & Ritchie, 2005; Sterckx et al., 2015). These experiences illustrate that maintaining public trust requires more than compliance with legal requirements. It also depends on meaningful public participation, transparency, and governance mechanisms that enable individuals to participate in decisions concerning the use of their health data. It is within this context that the UK has increasingly explored participatory gov-

ernance approaches, including data trusts, as mechanisms for strengthening accountability and rebuilding public confidence.

The basic principle underlying the data trust model is that there should be an independent stewardship structure where data governance can be inclusive and respectful to multiple interests (Paprica et al., 2020). Data trusts also seek to provide anticipatory governance of data while making trustworthy decisions about who has access to the data, the conditions for access, and who it benefits. Data trusts can therefore be recognized as an example of participatory governance which is characterized by practices of public engagement through a deliberative process or processes (Paprica et al., 2020).

B. Governance Structure and Operation of Data Trusts

There is currently no framework that prescribes the form that a data trust must take. They may therefore be established through different legal structures depending on the jurisdiction and the objectives they seek to achieve. Consequently, the term 'data trust' refers less to a specific legal entity than to a governance model characterized by common institutional features (Milne et al., 2021). They have also been described as organizations enabling data sharing by providing organizational and technical platforms. Typically, a data trust comprises four core elements. First, it identifies the datasets to be managed, which may include personal or anonymized health data contributed by individuals or organizations (Milne et al., 2021). Secondly, it appoints one or more independent trustees or stewards who assume fiduciary responsibilities for managing that data in accordance with the trust's governing rules rather than their own interests (The GPAI Data Governance Working Group, 2021). Thirdly, it establishes a governance framework, usually through a trust charter or equivalent instrument, which defines the trust's objectives, ethical principles, conditions governing access to data, decision-making procedures, rights of data contributors, mechanisms for withdrawal, benefit-sharing arrangements, and

accountability measures (The GPAI Data Governance Working Group, 2021). Finally, it identifies the beneficiaries, who may include data contributors, researchers, healthcare institutions, and, more broadly, the public, depending on the trust's stated purpose (Milne et al., 2021). Although individual data trusts differ in their legal form and operational arrangements, a key feature of the data trust model, aligned with participatory governance principles, is its focus on transparent and accountable interaction with stakeholders who participate as interested parties rather than trustees of the data trust, especially the individuals whose data are collected or affected (Milne et al., 2021).

C. Implementation of Data Trusts in the UK

Historically, the secondary use of health data within the UK has been governed through a combination of explicit consent for participation in specific research projects and the use of anonymized datasets without requiring individual consent or providing an opt-out mechanism. However, the rise of Big Data, major advances in data science, and the wider datafication of healthcare, together with recent legal and policy reforms, have created a much more complicated situation (Kerasidou & Kerasidou, 2023). These changes have raised concerns about how healthcare data is used and the kinds of data-sharing practices being adopted. In recent years, these concerns have contributed to several policy decisions that proved costly both financially and in terms of public trust.

These concerns first became evident during the implementation of the *care.data* program. Introduced in 2013, the program sought to extract patient information from general practice records for planning and research purposes. However, widespread criticism over inadequate public engagement and insufficient transparency regarding how the data would be used resulted in more than one million people opting out once the opportunity became available, ultimately leading to the program's cancellation in 2016 (Vezyridis, 2024). Many commentators attributed the

program's failure to the government's inability to communicate clearly the purposes, safeguards, and public benefits associated with the initiative, rather than to public opposition to data sharing itself (Vezyridis, 2024).

A similar pattern emerged in the UK in 2021 following the introduction of the General Practice Data for Planning and Research (GPDPR) program. The initiative proposed the sharing of NHS general practice data to support research and healthcare planning, including collaboration with private sector organizations undertaking health research and innovation. However, concerns relating to transparency, commercial access, patient control, and the absence of meaningful public consultation quickly resurfaced (Kerasidou & Kerasidou, 2023). Within weeks of the program's announcement, more than one million patients had opted out of data sharing, prompting the government to suspend implementation while undertaking further public engagement (Burki, 2021). Although the program remains under consideration, the controversy demonstrated that technical safeguards alone are insufficient where the public lacks confidence in the institutions responsible for managing health data.

The repeated failures of both the *care.data* and GPDPR programs prompted a broader reconsideration of health data governance within the UK. Rather than viewing public participation as a procedural requirement, policymakers increasingly recognized that sustained public confidence depends upon meaningful participation in decisions concerning the collection, use, and sharing of health data (Bartlett et al., 2024).

This shift is reflected in policy initiatives such as the *Data Saves Lives* strategy and the *10-Year Health Plan for England*, both of which identify transparency, accountability, and public participation as fundamental principles of health data governance (NHS England, 2023).

To operationalize these commitments, the Department of Health and Social Care, together with NHS England, established an extensive program of public deliberation. The program

incorporates nationally representative deliberative surveys, engagement with seldom-heard communities, independent oversight mechanisms, and ongoing public consultation on matters relating to secure data environments, the Single Patient Record, secondary uses of general practice data, and the linkage of health and non-health datasets (NHS England, 2023). Complementing these initiatives is the Health and Social Care Data Public Panel, comprising patients and members of the public who provide continuing advice on national health data policies and programs. These initiatives reflect an increasing recognition that legitimacy in health data governance depends not only upon legal compliance but also upon continuous public involvement in decision-making (NHS England, 2023).

Alongside these public engagement initiatives, the UK has also explored data trusts as an innovative governance model for the responsible stewardship of health data. The concept of data trusts was first introduced in the 2017 report '*Growing the Artificial Intelligence Industry in the UK*,' where they were proposed as institutions capable of facilitating responsible data sharing in the public interest. Their application within healthcare has continued to gain prominence over the years. One of the most significant contributions to this discussion is the General Practice Data Trust Pilot Study (GPDT) conducted by Redhead et al. (2024). The study explored whether a data trust could provide an appropriate governance framework for the collection, management, and sharing of general practice health data. Rather than focusing solely on legal or technical safeguards, the researchers engaged patients and members of the public to understand the underlying reasons behind widespread opposition to previous NHS data-sharing initiatives. The study found that participants were not fundamentally opposed to the secondary use of health data. Instead, they expressed concerns regarding transparency, accountability, commercial access to NHS data, and the absence of meaningful public involvement in decisions concerning data use (Redhead et al., 2024).

The findings reinforce broader scholarship arguing that public trust is strengthened where individuals are afforded genuine opportunities to participate in deliberations concerning the governance of their data rather than merely being consulted after decisions have already been made (Bartlett et al., 2024).

Building upon these findings, Redhead et al. (2024) proposed that a data trust could be established through the legal framework of a charitable trust, enabling trustees to exercise fiduciary responsibilities in the public interest while independently overseeing decisions concerning access to and use of health data. Similar proposals have been advanced by Bowden et al. (2026), who argue that charitable trusts provide a comprehensive governance mechanism capable of balancing the protection of individual rights with the societal benefits derived from health research. Other scholars have suggested alternative institutional arrangements capable of performing data trust functions without necessarily establishing a formal legal trust. Milne et al. (2024), for example, advocate for independent advisory committees and participant governance panels that incorporate patients, community representatives, and other stakeholders into decisions concerning data access and secondary uses of health information. Similar governance arrangements have long been utilized within biobanks to strengthen public confidence and improve accountability. Regardless of the institutional form adopted, these authors emphasize that participants' roles, powers, and responsibilities must be clearly defined, with genuine influence over decision-making rather than merely symbolic representation (Milne et al., 2024).

Despite growing interest in data trusts, significant challenges remain regarding their implementation within the UK. Scholars caution that poorly designed governance structures risk becoming tokenistic mechanisms that create the appearance of public participation without enabling meaningful deliberation or influencing decision-making (Milne et al., 2024). Questions also remain regarding the legal accountability of data trustees, par-

ticularly where governance failures result in privacy breaches or misuse of sensitive health information. Delacroix and Lawrence (2019) further observe that although fiduciary duties may establish high standards of conduct for trustees, these obligations alone may provide limited practical protection where trustees lack sufficient resources to compensate individuals harmed by negligent data management.

Consequently, effective implementation of data trusts requires not only robust governance structures but also clear accountability mechanisms, independent oversight, and enforceable legal remedies.

Although the precise legal structures proposed within the United Kingdom cannot be transplanted directly into Kenya, the UK experience nevertheless provides valuable lessons for strengthening participatory health data governance. In particular, it demonstrates that meaningful public engagement, transparent governance arrangements, and independent stewardship are essential for building public trust and securing the social legitimacy necessary for responsible health data sharing.

V. AN ANALYSIS OF PUBLIC TRUST AND PARTICIPATORY GOVERNANCE IN KENYA'S HEALTHCARE SYSTEM

An effective healthcare system is one where the people trust that practitioners and stakeholders will meet their medical needs and act in their best interests (Gicharu, 2023). The Kenyan health system has unfortunately been on an uneven footing for a long time because of general inaccessibility and the expensive nature of health services for a majority of Kenyans (Gicharu, 2023). Kenya's pursuit of universal healthcare has evolved for over thirty years through incremental reforms (Oyugi, 2024). The boldest of all has been an overhaul of the healthcare system under BETA, which introduced a comprehensive restructuring of the health sector through legislation, including the DHA. Collectively, these reforms seek to improve healthcare delivery while

supporting the country's transition towards a digitally integrated healthcare system capable of leveraging health information to improve healthcare planning, research, and service delivery (Oyugi, 2024).

The digitalization of Kenya's healthcare system has significantly increased the collection, storage, and exchange of electronic health information. The growing adoption of electronic medical records across healthcare facilities presents substantial opportunities for improving clinical care, disease surveillance, healthcare planning, and medical research (Mbuthia et al., 2019). At the same time, however, these developments have generated important governance questions concerning who should determine how health data is used, shared, and accessed, particularly where such uses extend beyond direct patient care.

These concerns have become increasingly apparent in the ongoing litigation challenging the Kenya–US Data Sharing Agreement. As discussed in chapter two of this paper, the proceedings raise broader questions regarding whether decisions involving the secondary use and cross-border sharing of health data can legitimately occur without meaningful public participation. Beyond the legal questions concerning data protection and privacy, the dispute illustrates the growing importance of public trust in determining the legitimacy of health data governance. It demonstrates that even where legal safeguards exist, public confidence may be undermined where affected communities perceive themselves to have been excluded from decisions concerning the use of their health information.

As discussed in the legislative framework section, Article 10 of the Constitution identifies public participation as one of the national values and principles of governance, while the Fourth Schedule devolves significant healthcare functions to county governments, thereby creating opportunities for citizen involvement in health decision-making. Within the healthcare sector, participatory governance seeks to ensure that citizens are actively involved in shaping health policies, priorities, and service

delivery rather than remaining passive recipients of healthcare services (Mugo et al., 2018). Such participation promotes transparency, accountability, and public ownership of healthcare decisions, thereby strengthening public trust in health institutions.

Despite this constitutional commitment, meaningful public participation within Kenya's health sector remains limited in practice. Researchers have observed that many citizens remain unaware of their opportunities to participate in health governance owing to inadequate civic education, limited access to information, and the absence of clearly established participatory structures at both national and county levels (The Star, 2024). Consequently, participation frequently occurs through ad hoc consultations rather than through institutionalized mechanisms capable of facilitating continuous dialogue between government institutions and the public. These shortcomings become even more pronounced in relation to the governance of health data. As demonstrated in the preceding legal analysis, the DHA establishes an extensive institutional and technical framework governing the collection, storage, protection, and exchange of health information.

However, the framework primarily conceptualizes individuals as data subjects whose interests are protected through consent requirements, privacy safeguards, and complaint mechanisms. It provides comparatively little opportunity for citizens to participate in broader decisions concerning secondary uses of health data, large-scale data integration, or cross-border data-sharing arrangements. It also fails to establish permanent public advisory bodies, citizen panels, or participatory oversight mechanisms through which patients and communities may influence decisions regarding the governance of health data. Consequently, the framework remains largely institution-driven, with decision-making concentrated within public authorities and health institutions.

Some valuable lessons may nevertheless be drawn from participatory governance initiatives implemented outside the formal

legislative framework. One such example is the work undertaken by the civil society organization Health Poverty Action (HPA), which examined participatory approaches to health governance across several African countries, including Kenya (Rolston et al., 2016). In Kenya, the project adopted a Community Conversations model designed to facilitate dialogue between community members, traditional leaders, religious leaders, and other stakeholders concerning health-related challenges. Although the initiative focused primarily on addressing Female Genital Mutilation, its participatory methodology offers useful insights for broader health governance. This methodology had a unique and contextually appropriate approach to encourage participation by marginal groups in health governance. The HPA Project used Community Conversations, similar to the UK's Health and Social Care Data Public Panel, as a communal dialogue and change process that allowed for the creation of a space that provided room for collective action (Rolston et al., 2016).

One of the lessons learned from the HPA Project in Kenya was that there was a need to create a careful balance between sharing and creating knowledge. This would ensure that there was space for communities and participants to create knowledge and new understandings of the healthcare system (Hulsen, 2020). The project also revealed that building trust and relationships is important. As the project was ongoing, facilitators convened groups of concerned community members who were willing to participate in the conversation.

In convening these groups, the facilitators took time to identify norms and rules for the conversations to ensure that all those who were involved were safe and comfortable (Rolston et al., 2016). This was done to ensure that there was trust between the facilitators and the participants.

The Community Conversations model demonstrated that meaningful participation extends beyond simply consulting members of the public. Rather, it involves creating sustained spaces for dialogue in which communities collectively develop knowledge,

deliberate on complex issues, and contribute to decision-making processes (Rolston et al., 2016). The project further highlighted the importance of building trust through carefully facilitated discussions that establish shared norms, encourage inclusive participation, and create safe environments in which participants feel able to express their views. Equally important was the role played by facilitators in ensuring that participation remained inclusive and meaningful. The project demonstrated that successful participatory governance depends upon facilitators who possess both technical knowledge and an understanding of institutional decision-making processes while also being capable of empowering communities to engage effectively (Ben Mesmia et al., 2023). At the same time, the project cautioned against reducing participation to periodic consultative meetings, noting that meaningful participation requires ongoing dialogue supported by informed citizens, accessible information, and institutional willingness to incorporate public perspectives into policy decisions (WHO, n.d.).

Kenya's current data governance system in the healthcare sector therefore illustrates both the growing recognition of public participation within the health sector and the significant institutional gaps that continue to exist. While constitutional principles strongly support public participation, existing governance mechanisms remain fragmented and largely focused on healthcare service delivery rather than the governance of health data. Unlike the UK, where public deliberation panels, citizen advisory structures, and pilot initiatives exploring data trusts have emerged in response to declining public trust, Kenya currently lacks comparable institutional mechanisms through which citizens can participate in decisions concerning the secondary use, integration, and sharing of health data.

As digital health systems continue to expand, strengthening participatory governance through institutionalized public engagement mechanisms will therefore be essential for fostering public trust and ensuring the long-term legitimacy of Kenya's health data governance framework.

The next section of this paper proposes a framework through which Kenya can strengthen participatory governance in health data management by drawing on lessons from the UK while adapting them to Kenya's constitutional, legal, and institutional context.

VI. THE WAY FORWARD FOR KENYA'S HEALTH DATA GOVERNANCE

The foregoing analysis demonstrates that while Kenya has made significant progress in establishing a legal and institutional framework for digital health, important gaps remain in relation to participatory governance and public trust owing to the fact that the current regime remains predominantly institution-driven with limited opportunities for citizens to participate meaningfully in shaping those decisions. Drawing from the comparative analysis of the UK and existing participatory initiatives within Kenya, this section proposes several recommendations that could strengthen participatory governance while remaining responsive to Kenya's constitutional and institutional context.

A. Embed Public Trust as a Guiding Principle of Health Data Governance

The first recommendation is that Kenya should expressly recognize public trust as a foundational principle underpinning health data governance. Public trust should not be regarded as a desirable outcome of effective regulation but rather as an objective that informs every stage of the collection, use, sharing, and governance of health data. This requires greater transparency regarding how health data is collected, who may access it, the purposes for which it is used, and the safeguards governing its protection. As demonstrated by the UK's experience with the *care.data* and GPDPR programs, the existence of legal authority to process health data does not necessarily generate public confidence where individuals perceive that important decisions are

being made without their involvement. Kenya should therefore ensure that future health data initiatives, including international data-sharing arrangements (Ministry of Health, 2025), are accompanied by continuous public engagement and accessible communication explaining the benefits, risks, and governance arrangements applicable to the data. In doing so, it is important to acknowledge that there exists a limitation in terms of the trust that people have in the healthcare system.

However, embedding public trust as a guiding principle also presents an important practical challenge. Much of the scholarship advocating trust-based models of health data governance has emerged from jurisdictions where public confidence in healthcare institutions and regulatory systems is comparatively higher than in many developing countries. In Kenya, levels of trust in the healthcare system have historically been undermined by challenges relating to inequitable access to healthcare, governance failures, and concerns regarding accountability (Gicharu, 2023). Public trust therefore cannot simply be presumed to exist or be created through legislative reform alone. Instead, it must be cultivated through consistent institutional practices that demonstrate transparency, accountability, and responsiveness to public concerns.

B. Amend the DHA to Establish a Health Data Advisory Council

Secondly, Kenya should amend the DHA to establish an independent Health Data Advisory Council under the Digital Health Agency. Rather than creating an entirely new institution, this Council would operate as an advisory and participatory body responsible for incorporating public perspectives into decisions concerning the governance and secondary use of health data. The Council should comprise representatives from patient organizations, healthcare professionals, county governments, civil society organizations, data protection experts, researchers, community representatives, and marginalized groups. Its mandate should include reviewing proposed secondary uses of health

data, advising on large-scale data-sharing initiatives, considering ethical concerns surrounding emerging digital health technologies, and facilitating continuous dialogue between government institutions and the public. Unlike the existing framework, where participation occurs primarily during the formulation of legislation or policy, the Advisory Council would institutionalize ongoing public participation throughout the lifecycle of health data governance. Such an amendment would operationalize the constitutional principle of public participation while strengthening transparency and accountability within the Digital Health Agency.

Nevertheless, the implementation of a data trust model should be approached with caution. Concentrating decision-making authority in trustees such as the Health Data Advisory Council may inadvertently create power imbalances, particularly where those entrusted with managing health data exercise broad discretion without meaningful public oversight (Gillwald, 2022). In contexts such as Kenya, where public awareness of data rights remains relatively limited and access to effective legal remedies may be constrained, there is a risk that data trustees could become the primary decision-makers without sufficient accountability to the communities whose interests they represent (The Commission on Administrative Justice (Office of the Ombudsman), 2025). This may reinforce existing information asymmetries and undermine, rather than strengthen, public trust (Gillwald, 2022).

C. Develop a Kenyan Model of Data Stewardship Informed by the Concept of Data Trusts

The third recommendation is that Kenya should gradually explore the adoption of a context-specific model of data stewardship informed by the principles underlying data trusts. Comparative analysis demonstrates that data trusts are not simply legal entities, but governance mechanisms designed to ensure that decisions regarding data sharing are made independently, trans-

parently, and in the public interest. Rather than transplanting the UK's charitable trust model directly into Kenya, policymakers should adapt the underlying principles to Kenya's legal and institutional framework. For example, the proposed Health Data Advisory Council could gradually perform governance functions associated with data trusts by independently reviewing proposed data-sharing arrangements, advising on public interest considerations, and ensuring that decisions concerning health data reflect the interests of patients and communities rather than solely institutional or commercial priorities. Such an approach would strengthen accountability while allowing Kenya to develop a participatory governance model consistent with its constitutional framework and existing institutional structures. Despite this, the adoption of a Kenyan model of data stewardship informed by data trusts should be approached cautiously. Data trusts remain an evolving governance model with no universally accepted legal or institutional structure. Further, establishing and maintaining such governance structures requires significant institutional capacity, financial resources, and continuous oversight.

D. Institutionalize Continuous Public Participation in Health Data Governance

Finally, Kenya should move beyond viewing public participation as a procedural requirement satisfied through occasional stakeholder consultations. Instead, participatory governance should be recognized as an ongoing process that accompanies the entire lifecycle of health data governance. The experiences of the Community Conversations implemented by Health Poverty Action demonstrate that meaningful participation requires continuous dialogue, civic education, trusted facilitators, and opportunities for communities to contribute to collective decision-making. Similar principles should guide health data governance. Achieving this objective will require sustained investment in civic education programs that improve public understanding of digital health, data protection rights, and the governance of

health information. Equally important is ensuring that communities receive feedback demonstrating how their participation has influenced institutional decisions, thereby reinforcing public confidence and strengthening accountability.

The institutionalization of participatory governance must, however, be approached pragmatically. The immediate priorities of many Kenyans remain centered on obtaining accessible, affordable, and quality healthcare services rather than participating in technical discussions concerning health data governance. Recent evidence indicates that most Kenyans are primarily concerned with their ability to obtain and afford healthcare, while many continue to experience difficulties accessing essential medicines and health services (Okello & Karimi, 2026). Consequently, participatory governance should be designed in a manner that respects these practical realities rather than assuming that all citizens possess the time, resources, or technical expertise to engage continuously in governance processes.

VII. CONCLUSION

Kenya has established an important constitutional, legislative, and institutional foundation for the digital transformation of its healthcare system. Nevertheless, the existing framework remains predominantly focused on regulating the technical and legal aspects of health data management, while providing limited mechanisms through which citizens can collectively influence decisions regarding the governance, sharing, and secondary use of their health data. In particular, the framework emphasizes individual consent and data protection rights rather than participatory structures that enable citizens to be represented in, or contribute to, decision-making processes concerning the use of health information for broader public, research, or commercial purposes. As digital health initiatives continue to expand, public trust will increasingly depend not only upon compliance with data protection obligations but also upon the extent to

which affected communities are meaningfully involved in shaping decisions concerning the use of their data. Drawing upon the comparative experience of the UK, this study demonstrates that participatory governance enhances transparency, accountability, and public confidence in health data governance. However, rather than advocating for the transplantation of foreign governance models, this study proposes that Kenya should develop context-specific mechanisms that build upon its existing constitutional and institutional framework.

In particular, amending the DHA, 2023 to establish a Health Data Advisory Council would provide an important first step towards institutionalizing public participation while laying the foundation for future governance models informed by the principles of data trusts.

REFERENCES

Aymé, S., Choquet, R., Devillers, L., Gilard, M., Kelly-Irving, M., Livartowski, A., & Lukacs, B. (2026). Benefits and Risks of Using Health Data for Research. Paris Brain Institute-ICM, 1(1). https://hal.science/hal-04371062v1/document

Baniulyte, G., Rogerson, N., & Bowden, J. (2023). Evolution – Removing Paper and Digitising the Hospital. Health and Technology, 13(2). https://doi.org/10.1007/s12553-023-00740-8

Bartlett, B., Ainsworth, J., Cunningham, J., Davidge, G., Harding, M., Holm, S., Neumann, V., & Devaney, S. (2024). Health data stewardship: achieving trust through accountability in health data sharing for research. *Law Innovation and Technology, 16(2), 1–41.* https://doi.org/10.1080/17579961.2024.2392937

Ben Mesmia, H., Rajan, D., Bouhafa Chtioui, R., Koch, K., Jaouadi, I., Aboutaleb, H., De Courcelles, S., Atmani, L., Pujos, B., & Mtiraoui, A. (2023). The Tunisian experience of participatory health governance: the Societal Dialogue for Health (a qualitative study). *Health Research Policy and Systems, 21(1), 84.* https://doi.org/10.1186/s12961-023-00996-6

Bernadette, A., Anthony, K., Ngaira, D., & Pepela, W. (2018). BRIEF POLICY Enhancing Health Information System for Evidence based decision making in the Health Sector Executive Statement. THE HEALTH SECTOR MONITORING AND EVALUATION UNIT - MINISTRY OF HEALTH, KENYA. http://guidelines.health.go.ke:8000/media/Health_Information_System_Policy_Brief_May_2018.pdf

Bowden, C., Devaney, S., Redhead, C., Ainsworth, J., Holm, S., & Cunningham, J. (2026). Conceptualising 'my data': Going beyond data security to build trustworthy governance of health data sharing. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.6580822

Burki, T. (2021). Concerns over England's new system for collecting general practitioner data. The Lancet Digital Health, 3(8), e469–e470. https://doi.org/10.1016/s2589-7500(21)00148-5

Cipesa.org. (2024, April). *What Does Kenya's Digital Health Act Portend for Data Governance and Regulation?* Cipesa; CIPESA. https://cipesa.org/wp-content/files/Policy_Brief_-_Kenyas_Digital_Health_Act.pdf

Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data Trusts: Disturbing the 'one size fits all' approach to data governance. International Data Privacy Law, 9(4). https://doi.org/10.1093/idpl/ipz014

Department of Health and Social Care. (2012, March 8). NHS Constitution for England. GOV.UK. https://www.gov.uk/government/publications/the-nhs-constitution-for-england

Doctors Explain Digital Health Co. LTD. (2025, April 25). *Abstract Digital health systems have increasingly become central to the transformation of healthcare services globally. Kenya, in particular, has shown significant strides toward digitizing its health infrastructure.* Linkedin.com. https://www.

linkedin.com/pulse/digital-health-systems-kenyan-hospitals-hits-misses-opportunities-21shf/

Field, O., Modhvadia, R., Pavel, V., & Patterson, L. (2024, December 13). Participatory and inclusive data stewardship. Adalovelaceinstitute.Org. https://www.adalovelaceinstitute.org/report/participatory-inclusive-data-stewardship/

FNIH. (2025). Patient engagement and patient-centricity: Considerations and best practices [Review of Patient engagement and patient-centricity: Considerations and best practices]. Document360.Io. https://bgtcplaybook.document360.io/docs/considerations-and-best-practices-for-patient-engagement-and-patient-centricity

Gicharu, P. G. (2023, July 25). *Trust is Crucial For Effective Healthcare To Kenyans*. CIO Africa. https://cioafrica.co/trust-is-crucial-for-effective-healthcare-to-kenyans/

Gillwald, A. (2022, May 5). Data trusts to support participatory data governance in South Africa? Research ICT Africa. https://researchictafrica.net/2022/05/05/data-trusts-to-support-participatory-data-governance-in-south-africa/

Hassan, A. (2025, January 10). Big Data in Healthcare: Uses, Benefits, Challenges, and Real Examples [Review of Big Data in Healthcare: Uses, Benefits, Challenges, and Real Examples]. MGH Institute of Health Professions. https://www.mghihp.edu/news-and-more/opinions/data-analytics/big-data-healthcare-uses-benefits-challenges-and-real-examples

Hulsen, T. (2020). Sharing Is Caring—Data Sharing Initiatives in Healthcare. *International Journal of Environmental Research and Public Health, 17(9), 3046*. https://doi.org/10.3390/ijerph17093046

Hummel, P., Braun, M., & Dabrock, P. (2020). Own Data? Ethical Reflections on Data Ownership. *Philosophy & Technology*, *34*. https://doi.org/10.1007/s13347-020-00404-9

Ireri, S., Waiganjo, P., Ochieng, D. O., Kagiri, M., Anindo, M., Adoyo, M., Wanjiru, R., Kirui, J., Pundo, R., Kimani, M., & Wanyungu, J. (2025). An exploration of the successful scale-up of the electronic community health information system in Kenya. *Oxford Open Digital Health*, *3*(1). https://doi.org/10.1093/oodh/oqaf020

Kariotis, T., Ball, M. P., Greshake Tzovaras, B., Dennis, S., Sahama, T., Johnston, C., Almond, H., & Borda, A. (2020). Emerging health data platforms: From individual control to collective data governance. *Data & Policy*, *2*. https://doi.org/10.1017/dap.2020.14

Kerasidou, A., & Kerasidou, C. (2023). Data-driven research and healthcare: public trust, data governance and the NHS. *BMC Medical Ethics*, *24*(1). https://doi.org/10.1186/s12910-023-00922-z

Li, Z., Shi, J., Li, N., Wang, M., Jin, Y., & Zheng, Z. (2022). Temporal trends in the burden of non-communicable diseases in countries with the highest malaria burden, 1990–2019: Evaluating the double burden of non-communicable and communicable diseases in epidemiological transition.

Globalization and Health, 18(1). https://doi.org/10.1186/s12992-022-00882-w

Macdonald, L., & Ritchie, A. (2005). Health on-line: public attitudes to data sharing in the NHS. https://www.statewatch.org/media/documents/news/2005/nov/scot-nhs-database.pdf

Mbuthia, D., Molyneux, S., Njue, M., Mwalukore, S., & Marsh, V. (2019). Kenyan health stakeholder views on individual consent, general notification and governance processes for the re-use of hospital inpatient data to support learning on healthcare systems. *BMC Medical Ethics*, *20*(1). https://doi.org/10.1186/s12910-018-0343-9

McKee, M., May, Greenley, R., & Govin Permanand. (2025). Trust and health systems. Nih.gov; European Observatory on Health Systems and Policies. https://www.ncbi.nlm.nih.gov/books/NBK618145/

Mears, D. (2014). *Classes of Charity: Overview*. https://www.russell-cooke.co.uk/media/xqcbiloz/classes-of-charity-westlaw-uk-july-2014cleaned.pdf

Milne, R., Sorbie, A., & Dixon-Woods, M. (2021). What can data trusts for health research learn from participatory governance in biobanks? *Journal of Medical Ethics*, *48*, medethics-2020-107020. https://doi.org/10.1136/medethics-2020-107020

Ministry of Health. (2016). *KENYA NATIONAL eHEALTH POLICY 2016-2030 Towards attainment of the highest standard of health through adoption and use of ICT MINISTRY OF HEALTH REPUBLIC OF KENYA*. https://extranet.who.int/countryplanningcycles/sites/default/files/public_file_rep/KEN_Kenya_National-eHealth-Policy_2016-2030.pdf

Ministry of Health. (2020). Kenya Universal Health Coverage Policy 2020 – 2030 . Ministry of Health. http://guidelines.health.go.ke:8000/media/Kenya_Universal_Health_Coverage_Policy_2020__2030.pdf

Ministry of Health. (2025). *Data Sharing Agreement signed between the Government of Kenya and the Government of the United States of America* . https://healthpolicy-watch.news/wp-content/uploads/2025/12/US-Kenya-Data-Sharing-Agreement.pdf

Mugo, P., Onsomu, E., Munga, B., Nafula, N., Mbithi, J., & Owino, E. (2018). *An Assessment of Healthcare Delivery in Kenya under the Devolved System*. KENYA INSTITUTE FOR PUBLIC POLICY RESEARCH AND ANALYSIS (KIPPRA) . https://kippra.or.ke/wp-content/uploads/2021/02/an-assessment-of-healthcare-delivery-in-kenya-under-the-devolved-system-sp19.pdf

Musoni, M., Pouyé , R., & Odhiambo, S. (2026). Digital public infrastructure in the East African Community. Https://Ecdpm.Org/Application/Files/5217/7685/8488/Digital-Public-Infrastructure-East-African-Community-ECDPM-Discussion-Paper-404-2026.Pdf

NG'ANG'A-KNA, J. (2026). Health Ministry begins transition to New SHA Digital Health System | Government Advertising Agency. Gaa.Go.Ke. https://gaa.go.ke/health-ministry-begins-transition-new-sha-digital-health-system

NHS England. (2023). National public engagement on the use of health and care data. https://digital.nhs.uk/data-and-information/keeping-data-safe-and-benefitting-the-public/national-public-engagement-in-the-use-of-health-and-care-data#top

OECD. (2015). Health Data Governance: Privacy, Monitoring and Research - Policy Brief. https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/health-data-governance_39fe6a69/54ba9d10-en.pdf

OECD. (2022). *Health Data Governance for the Digital Age IMPLEMENTING THE OECD RECOMMENDATION ON HEALTH DATA GOVERNANCE*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/05/health-data-governance-for-the-digital-age_5c42de41/68b60796-en.pdf

Okello, A., & Karimi, E. (2026). AD1120: Kenyans see health as a key priority for government action, endorse universal access. Afrobarometer.Org. https://www.afrobarometer.org/publication/ad1120-kenyans-see-health-as-a-key-priority-for-government-action-endorse-universal-access/

Oware, P. M., Omondi, G., Adipo, C., Adow, M., Wanyama, C., Odallo, D., Bosire, N., Okong'o, L., Maina, M., Aluvaala, J., Ngwatu, P., Githanga, D., Kinuthia, D., Amadi, I., Rukwaro, G., Kerubo, L., Amisi, C., Govoga, A., Karimi, J., & Kahtra, A. (2025). Perceived accuracy and utilisation of DHIS2 data for health decision making and advocacy in Kenya: A Qualitative Study. *PLOS Global Public Health*, *5*(8), e0004508. https://doi.org/10.1371/journal.pgph.0004508

Oyugi, B. (2024, October 10). *Kenya is overhauling its national healthcare scheme after 58 years – what would make the transition less painful*. The Conversation. https://theconversation.com/kenya-is-overhauling-its-national-healthcare-scheme-after-58-years-what-would-make-the-transition-less-painful-240963

Paprica, P. A., Sutherland, E., Smith, A., Brudno, M., Cartagena, R. G., Crichlow, M., Courtney, B., Loken, C., McGrail, K. M., Ryan, A., Schull, M. J., Thorogood, A., Virtanen, C., & Yang, K. (2020). Essential Requirements for Establishing and Operating Data Trusts. International Journal of Population Data Science, 5(1). https://doi.org/10.23889/ijpds.v5i1.1353

Piasecki, J., & Cheah, P. Y. (2022). Ownership of individual-level health data, data sharing, and data governance. *BMC Medical Ethics*, *23*(1). https://doi.org/10.1186/s12910-022-00848-y

Redhead, C. A. B., Bowden, C., Ainsworth, J., Burns, N., Cunningham, J., Holm, S., & Devaney, S. (2024). Unlocking the promise of UK health data: Considering the case for a charitable GP data trust. *Medical Law Review*, *33*(1). https://doi.org/10.1093/medlaw/fwae043

Rolston, I. A., Edwards, S., Tobin, N., Nizeyimana, M., Yego, B., & Steenkamp, P. (2016). *Participatory Governance: Sharing best practices for the participation of marginalised groups in health sector governance*. Health Poverty Action. https://www.healthpovertyaction.org/wp-content/uploads/2025/01/Paricipatory-Governance-web-version-2016.pdf

Souvatzi, E., Katsikidou, M., Arvaniti, A., Plakias, S., Tsiakiri, A., & Samakouri,

M. (2024). Trust in Healthcare, Medical Mistrust, and Health Outcomes in Times of Health Crisis: A Narrative Review. *Societies*, *14*(12), 269–269. https://doi.org/10.3390/soc14120269

Sterckx, S., Rakic, V., Cockbain, J., & Borry, P. (2015). 'You hoped we would sleep walk into accepting the collection of our data': controversies surrounding the UK care.data scheme and their wider relevance for biomedical research. *Medicine, Health Care and Philosophy*, *19*(2), 177–190. https://doi.org/10.1007/s11019-015-9661-6

The Commission on Administrative Justice (Office of the Ombudsman). (2025, May). Assessing the right of Access to information implementation in Kenya. https://www.ombudsman.go.ke/sites/default/files/202603/Kenya%20ATI%20Assessment%20Report%202025.pdf

The GPAI Data Governance Working Group. (2021). Understanding Data Trusts. https://datatrusts.uk/assets/pdfs/2021-07-09-GPAI-summary-understanding-data-trusts-updated.docx.pdf

The Star. (2024). *New policy exposes challenges facing effective public participation. The Star*. https://www.the-star.co.ke/sasa/lifestyle/2024-06-22-new-policy-exposes-challenges-facing-effective-public-participation

Tiffin, N., George, A., & LeFevre, A. E. (2019). How to use relevant data for maximal benefit with minimal risk: digital health data governance to protect vulnerable populations in low-income and middle-income countries. *BMJ Global Health*, *4*(2), e001395. https://doi.org/10.1136/bmjgh-2019-001395

Transform Health. (2022). HEALTH DATA GOVERNANCE PRINCIPLES [Review of HEALTH DATA GOVERNANCE PRINCIPLES]. https://healthdatagovernance.org/wp-content/uploads/2024/11/EN-Health-Data-Governance-Principles-1.pdf

Transform Health. (2024). *Model Law on Health Data Governance*. Https://Transformhealthcoalition.org/; Transform Heealth. https://healthdatagovernance.org/wp-content/uploads/2025/01/Model-Law-on-Health-Data-Governance-Jan-25.pdf#:~:text=that%20can%20arise%20from%20principles,health%20data%20ethically%20and%20responsibly

Unver, M. B., & Odusola-Stevenson, S. (2025). UK AI Governance at a Crossroads: Charting the Path Ahead. International Journal of Mass Communication, 3, 168–183. https://doi.org/10.6000/2818-3401.2025.03.12

Vezyridis, P. (2024). 'Kindling the fire' of NHS patient data exploitations: The care.data controversy in news media discourses. *Social Science & Medicine*, *348*, 116824–116824. https://doi.org/10.1016/j.socscimed.2024.116824

Walubengo, J. (2023, October 24). *Kenya's Digital Health Act: A Leap Forward in Data Governance | KICTANet Think Tank*. KICTANet. https://www.kictanet.or.ke/kenyas-digital-health-act-a-leap-forward-in-data-governance/

WHO. (2021). Ethical Considerations and Data Protection Principles. Who.Int. https://smart.who.int/trust/1.1.4/ethical_principles.html

WHO. (n.d.). *Promoting participatory governance social participation and accountability. Www.who.int. https://www.who.int/activities/promoting-participatory-governance-social-participation-and-accountability-Wilde, D., & Moore, I. (2021). Charitable relief of financial hardship: The public benefit requirement. Central Archive at the University of Reading.* https://centaur.reading.ac.uk/95528/3/22Jan2021Charitable%20Relief%20of%20Financial%20Hardship%20-%20the%20Public%20Benefit%20Requirement.pdf