International Journal of Humanities, Management, Engineering, Education and Legal studies

Biometric Identity, Privacy Rights, and Refugee Protection: Legal Challenges in Africa's Digital ID Revolution

Prof (Dr) Daniel Mairafi Gimbason, Head of Department, Health Sciences, Nasarawa State University, Keffi, Nasarawa State, Nigeria

Abstract

The proliferation of biometric digital identity systems across Africa presents a complex intersection of technological innovation, human rights protection, and refugee welfare. This paper examines the legal and ethical challenges emerging from Africa's rapid adoption of biometric identification technologies, particularly concerning refugee populations who face unique vulnerabilities in digital identity ecosystems. Through comprehensive analysis of regulatory frameworks, case studies from multiple African nations, and international human rights law, this research reveals significant gaps between technological implementation and legal protection mechanisms. The study demonstrates that while biometric systems offer unprecedented opportunities for service delivery and identity verification, they simultaneously create substantial risks to privacy rights, data security, and refugee protection. Drawing on empirical evidence from Kenya, Uganda, South Africa, and regional biometric initiatives, this paper identifies critical legal challenges including inadequate data protection legislation, surveillance concerns, and the potential for discriminatory exclusion. The findings underscore the urgent need for harmonized legal frameworks that balance technological advancement with fundamental human rights, particularly for displaced populations who depend on these systems for accessing essential services and legal protections.

Keywords: Biometric identification, digital identity, refugee protection, data privacy, human rights, Africa, GDPR, UNHCR, digital exclusion, surveillance

1. Introduction

The African continent stands at the forefront of a digital identity revolution that promises to transform governance, service delivery, and social inclusion while simultaneously raising profound questions about privacy rights and human dignity. Over the past decade, more than thirty African countries have implemented or are developing national biometric identity systems, driven by aspirations to formalize populations, enhance security, improve service delivery, and facilitate financial inclusion (Gelb & Metz, 2018). These systems capture unique biological characteristics such as fingerprints, iris patterns, and facial features, creating digital representations of identity that governments and international organizations increasingly treat as prerequisites for accessing fundamental rights and services.

For refugee populations across Africa, which numbered approximately 7.3 million by 2024 according to United Nations High Commissioner for Refugees statistics, biometric identification systems represent both opportunity and peril. On one hand, digital identity can provide displaced persons with documentation that facilitates access to humanitarian assistance, education, healthcare, and formal employment opportunities that might otherwise remain inaccessible (Jacobsen, 2015). The ability to establish and verify identity through biometric means offers refugees a pathway toward recognition and social integration in host countries where traditional documentation may be absent, destroyed, or unrecognized.

On the other hand, the collection, storage, and sharing of biometric data creates unprecedented vulnerabilities for populations already marginalized by displacement, statelessness, and legal precarity. Unlike passwords or identification cards, biometric identifiers cannot be changed if compromised, making data breaches potentially catastrophic for individuals whose safety may depend on anonymity or whose persecution may intensify if their location or identity becomes known to hostile actors (Madianou, 2019). The permanent nature of biometric data, combined with inadequate legal protections in many African jurisdictions, creates conditions where the very systems designed to protect and include refugees may instead expose them to surveillance, discrimination, and harm.

The legal landscape governing biometric identity systems in Africa remains fragmented and underdeveloped relative to the technological capabilities being deployed. While the European Union's General Data Protection Regulation (GDPR) and similar comprehensive frameworks provide robust protections for biometric data in other regions, most African countries operate with outdated data protection laws that predate biometric technologies or lack enforceable privacy regulations entirely (Greenleaf, 2020). This regulatory deficit becomes particularly acute in contexts involving refugees, who may lack the legal standing, information, or resources necessary to challenge data processing practices or seek remedies for violations.

The African Union's Convention on Cyber Security and Personal Data Protection, adopted in 2014 but ratified by only a minority of member states, represents an ambitious attempt at regional harmonization that has yet to achieve widespread implementation. Meanwhile, international frameworks such as the United Nations' Sustainable Development Goal 16.9, which calls for legal identity for all by 2030, create pressure for rapid biometric enrollment without necessarily ensuring adequate safeguards (Breckenridge, 2014). This gap between technological implementation and legal protection generates what scholars have termed a "regulatory vacuum" where fundamental rights remain vulnerable to state and corporate interests in data extraction and surveillance.

This paper examines the legal challenges at the intersection of biometric identity systems, privacy rights, and refugee protection across Africa. Through analysis of national legislation, regional frameworks, international human rights law, and empirical case studies, this research identifies critical tensions between technological innovation and human rights protection. The study focuses on three primary research questions: First, what legal frameworks currently govern biometric data collection and processing in African countries hosting significant

refugee populations? Second, how do these frameworks align with or diverge from international human rights standards, particularly regarding privacy, data protection, and refugee rights? Third, what legal reforms or interventions are necessary to ensure that digital identity systems serve rather than undermine refugee protection?

The significance of this research extends beyond academic inquiry to urgent policy implications for governments, international organizations, humanitarian agencies, and civil society actors engaged in identity system development and refugee protection. As biometric technologies become increasingly ubiquitous across Africa and globally, the legal frameworks established today will shape the relationship between individuals and states, citizens and governments, for generations to come. For refugees whose survival and dignity often depend on the protection afforded by legal systems, the stakes of this digital revolution could not be higher.

2. Biometric Identity Systems in Africa: Technological Context and Proliferation

The rapid expansion of biometric identification infrastructure across Africa represents one of the continent's most significant technological transformations in the early twenty-first century. Biometric systems utilize unique physiological or behavioral characteristics to identify and authenticate individuals, with fingerprint recognition, iris scanning, and facial recognition technologies being the most commonly deployed modalities in African contexts (Breckenridge, 2014). The technological architecture typically includes enrollment stations where biometric data is captured, centralized databases where this information is stored, and verification systems that match presented biometric samples against stored templates. The scale and sophistication of these systems vary considerably across countries, ranging from basic fingerprint databases to advanced multimodal systems integrating multiple biometric identifiers with demographic information.

Nigeria's National Identity Management Commission, established in 2007, oversees one of Africa's largest biometric enrollment initiatives, which had registered over 90 million citizens by 2023 despite ongoing challenges with coverage and accuracy (Adeyemi, 2021). The Nigerian system captures ten fingerprints and facial images, linking this biometric data to a unique National Identification Number intended to serve as the foundation for accessing government services, opening bank accounts, obtaining mobile phone SIM cards, and verifying identity for security purposes. Similarly, Kenya's Huduma Namba system, launched in 2019, aimed to consolidate multiple identification documents into a single biometric-enabled national ID that would streamline service delivery and enhance security, though its implementation has been contested in courts due to privacy concerns (Namwaya, 2020).

South Africa's Home Affairs National Identification System represents one of the continent's more mature biometric infrastructures, having incorporated fingerprint biometrics since the late 1990s and progressively expanded to include facial recognition capabilities. The system processes approximately 1.2 million identity document applications annually and maintains biometric records for both citizens and documented foreign nationals, including refugees with formal status (Breckenridge, 2014). Ghana's National Identification Authority completed a

comprehensive biometric registration exercise between 2017 and 2020, issuing Ghana Cards to over 15 million residents and establishing biometric verification systems integrated with banking, telecommunications, and government services (Nikoi, 2022).

The technological infrastructure supporting these systems increasingly relies on cloud computing, artificial intelligence, and interoperable databases that facilitate data sharing across government agencies and potentially with private sector entities. Rwanda's national ID system exemplifies this trend toward digital integration, with biometric identifiers serving as authentication mechanisms for services ranging from health insurance to land registration and mobile money transactions (Mann & Daly, 2019). The Rwandan approach reflects a broader continental shift toward "digital government" models where biometric identity becomes the foundational layer for accessing an expanding array of digital services and platforms.

Regional initiatives have emerged alongside national systems, creating additional layers of biometric data collection and processing. The Economic Community of West African States (ECOWAS) biometric passport and identity card system aims to facilitate regional mobility while establishing shared standards for identity verification across fifteen member countries. The East African Community has similarly pursued harmonized biometric identity frameworks intended to support free movement and regional integration, though implementation remains uneven across member states (Donovan, 2015). These regional systems create complex questions about data governance, particularly regarding which entities exercise control over biometric databases and how information flows across national boundaries.

For refugee populations, biometric identity systems operate at multiple levels simultaneously. Host country national identification systems may include refugees, exclude them, or maintain separate registration processes depending on national legal frameworks and policy choices. Kenya's national ID system formally excludes refugees and asylum seekers, relegating them to separate documentation managed by the Department of Refugee Affairs and UNHCR, while countries like Uganda have moved toward including refugees in national identification systems as part of progressive refugee policies (Omata, 2020). This variation in approach creates significant disparities in refugees' ability to access services, work legally, and integrate into host communities.

The United Nations High Commissioner for Refugees has independently developed and deployed the Biometric Identity Management System (BIMS), which operates in refugee camps and urban refugee contexts across Africa. By 2023, UNHCR's biometric database contained records for more than 8 million individuals globally, with substantial portions in African countries including Kenya, Ethiopia, Uganda, Tanzania, and South Sudan (UNHCR, 2022). The BIMS system captures fingerprints and iris scans, linking this biometric data to demographic information and case files that document refugees' legal status, family relationships, and assistance entitlements. UNHCR presents biometric registration as essential for preventing fraud, ensuring equitable distribution of assistance, protecting vulnerable individuals, and supporting resettlement processes.

However, the proliferation of parallel biometric systems creates what researchers have termed "datafication of displacement," where refugees become subject to multiple overlapping regimes of biometric surveillance and control (Madianou, 2019). A single refugee family in Kenya, for example, may be enrolled in UNHCR's BIMS system, Kenya's Refugee Affairs Secretariat registration database, World Food Programme biometric verification systems for food assistance, and potentially biometric systems operated by non-governmental organizations providing health, education, or livelihood services. Each enrollment creates additional data points, increases exposure to potential breaches, and generates concerns about how information might be shared, combined, or used for purposes beyond the original collection context.

The technological capabilities embedded in contemporary biometric systems extend far beyond simple identity verification. Advanced facial recognition algorithms can perform continuous surveillance, identifying individuals in crowds or tracking their movements across multiple camera systems. Fingerprint databases enable rapid cross-referencing that can link individuals to criminal records, immigration violations, or other government databases. Iris recognition systems can authenticate identity even when other identifying documents are absent or contested (Gates, 2011). These capabilities create powerful tools for law enforcement and border control, but they simultaneously create infrastructures of surveillance that can be deployed against vulnerable populations, including refugees fleeing persecution.

The accuracy and reliability of biometric technologies vary substantially based on factors including the quality of enrollment equipment, environmental conditions during capture, the algorithms used for matching, and the demographic characteristics of enrolled populations. Research has documented higher error rates in fingerprint recognition for manual laborers whose fingerprints may be worn or damaged, in iris recognition for individuals with certain eye conditions, and in facial recognition for individuals with darker skin tones due to algorithmic bias (Buolamwini & Gebru, 2018). For refugees who may have experienced physical trauma, malnutrition, or harsh environmental conditions that affect their biometric characteristics, these accuracy limitations can result in denial of services or inability to verify identity when needed.

3. Legal Frameworks Governing Biometric Data in Africa

The legal architecture governing biometric data protection across Africa presents a fragmented landscape characterized by substantial variation in legislative comprehensiveness, enforcement capacity, and alignment with international human rights standards. As of 2024, fewer than half of African countries had enacted dedicated data protection legislation, and among those with legal frameworks in place, provisions specifically addressing biometric data as a sensitive category requiring heightened protection remain inconsistent (Greenleaf, 2020). This regulatory gap becomes particularly problematic given the irreversible nature of biometric identifiers and the profound privacy implications associated with their collection, storage, and processing.

South Africa's Protection of Personal Information Act (POPIA), which came into full effect in 2021, represents one of the continent's most comprehensive data protection frameworks. The legislation explicitly classifies biometric information as a special category of personal information subject to stringent processing conditions including requirements for explicit consent, limitations on purpose, and enhanced security measures (Roos, 2021). POPIA establishes an Information Regulator with enforcement powers including the ability to issue compliance orders, conduct investigations, and impose penalties for violations. However, the Act contains broad exemptions for processing conducted in the interests of national security or for law enforcement purposes, creating potential loopholes that may undermine protections for vulnerable populations including refugees.

Kenya's Data Protection Act of 2019 similarly recognizes biometric data as sensitive personal data requiring heightened protections, mandating that data controllers obtain explicit consent before processing such information and implement appropriate security measures to prevent unauthorized access or breaches. The Kenyan framework establishes a Data Protection Commissioner with investigative and enforcement authority, and it provides data subjects with rights including access to their information, correction of inaccuracies, and objection to processing in certain circumstances (Namwaya, 2020). Critically, the Act requires that data processing adhere to principles of lawfulness, fairness, transparency, purpose limitation, and data minimization, establishing standards that should govern biometric identity systems.

Despite these legal protections on paper, implementation of Kenya's Data Protection Act has revealed significant challenges particularly regarding biometric systems already deployed prior to the legislation's enactment. The Huduma Namba national identification system became the subject of litigation shortly after its launch, with petitioners arguing that the mandatory biometric enrollment violated constitutional rights to privacy and that the system lacked adequate legal framework governing data collection, storage, sharing, and security (Nubian Rights Forum & Others v Attorney General & 6 Others, 2020). Kenya's High Court temporarily suspended full implementation pending assessment of privacy impact and establishment of proper safeguards, illustrating the tension between rapid technological deployment and legal protection requirements.

Uganda's Data Protection and Privacy Act of 2019 establishes a regulatory framework that includes provisions for biometric data protection, though the legislation's effectiveness has been questioned given Uganda's extensive deployment of surveillance technologies and limited institutional capacity for enforcement. The Ugandan framework requires data controllers to register with the National Information Technology Authority and to implement security measures protecting personal data, but enforcement mechanisms remain underdeveloped and awareness of legal rights among refugee populations is minimal (Unwanted Witness, 2021). Uganda's progressive refugee policies, which formally include refugees in national identification systems and extend work rights, create a context where biometric data governance becomes particularly critical for protecting displaced populations' interests.

The African Union Convention on Cyber Security and Personal Data Protection, adopted in 2014 and commonly referred to as the Malabo Convention, represents the most ambitious attempt at regional harmonization of data protection standards. The Convention establishes principles for personal data processing that align broadly with international standards including requirements for consent, purpose limitation, data quality, security, and accountability. Article 14 specifically addresses sensitive personal data, though it does not explicitly enumerate biometric information within this category, potentially creating ambiguity about the level of protection required (African Union, 2014). As of 2024, the Convention had been ratified by only fifteen African Union member states and had not yet achieved the threshold for entry into force, limiting its practical impact on biometric data governance across the continent.

Nigeria's Data Protection Regulation of 2019, issued by the National Information Technology Development Agency, provides a framework for personal data protection that includes principles of consent, lawfulness, and data security. However, the Regulation's status as an administrative directive rather than parliamentary legislation raises questions about its legal force and enforceability, particularly in contexts where government agencies assert competing interests in data access for security or administrative purposes (Adeyemi, 2021). Nigeria's deployment of a national biometric identity system proceeded largely without specific privacy impact assessments or public consultation about data governance, reflecting a common pattern across Africa where technological implementation precedes rather than follows legal framework development.

Ghana's Data Protection Act of 2012, one of Africa's earlier comprehensive data protection laws, establishes a Data Protection Commission with regulatory and enforcement authority. The Act recognizes sensitive personal data as a category requiring additional protections, though its specific application to biometric information has evolved through regulatory guidance rather than explicit statutory provisions (Nikoi, 2022). Ghana's National Identification Authority has issued assurances about security measures and data protection compliance in its biometric enrollment system, but independent verification of these claims and mechanisms for accountability remain limited.

Regional economic communities have developed data protection frameworks that apply to member states, creating additional layers of legal architecture governing biometric systems. The Economic Community of West African States adopted a Supplementary Act on Personal Data Protection in 2010, establishing principles for lawful data processing and creating obligations for data controllers to implement security measures and respect data subjects' rights. The East African Community has similarly pursued harmonized data protection standards through its Model Data Protection Law, though implementation across member states remains incomplete and uneven (Donovan, 2015).

International human rights frameworks provide additional legal foundations for challenging biometric data practices that violate privacy rights or other fundamental protections. The International Covenant on Civil and Political Rights, to which most African countries are

parties, enshrines the right to privacy in Article 17, protecting individuals against arbitrary or unlawful interference with their privacy, family, home, or correspondence. The African Charter on Human and Peoples' Rights recognizes privacy rights under Article 4 and has been interpreted by the African Commission on Human and Peoples' Rights to encompass protection against surveillance and data collection that threaten individual dignity and autonomy (Manby, 2016).

For refugee populations specifically, the 1951 Refugee Convention and its 1967 Protocol establish legal standards that constrain states' treatment of refugees, including obligations to provide identity documents and travel papers, prohibitions on penalizing refugees for illegal entry, and limitations on expulsion except on grounds of national security or public order. The principle of non-refoulement, codified in Article 33, prohibits returning refugees to territories where their lives or freedom would be threatened, creating obligations that extend to data protection contexts where biometric information might be shared with countries of origin or other actors who pose threats to refugees (Goodwin-Gill & McAdam, 2021). The confidentiality of information concerning refugees is recognized as essential to protection, yet biometric databases create potential vulnerabilities that challenge this principle.

The African Union Convention Governing the Specific Aspects of Refugee Problems in Africa, adopted in 1969, expands refugee protection beyond the 1951 Convention definition and emphasizes the voluntary nature of repatriation and the security of refugees in host countries. These protection obligations should inform biometric data governance, requiring that digital identity systems incorporate safeguards preventing data sharing that could compromise refugees' safety or expose them to risks in countries of origin (Sharpe, 2018). However, explicit connections between refugee protection principles and biometric data governance remain underdeveloped in most national legal frameworks.

The legal principle of informed consent, central to data protection frameworks globally, presents particular challenges in refugee contexts where power imbalances, information asymmetries, and dependencies on assistance create conditions where consent may not be truly voluntary or informed. Refugees facing food insecurity may have little practical choice but to submit to biometric enrollment if assistance distribution depends on verification through these systems. Language barriers, limited literacy, and inadequate explanation of data processing practices further compromise the meaningfulness of consent in many refugee contexts (Jacobsen, 2015). Legal frameworks that rely primarily on consent as the basis for lawful processing may therefore prove inadequate for protecting refugee populations' rights.

4. Privacy Rights and Data Protection Challenges in Biometric Systems

The deployment of biometric identification systems across Africa creates profound challenges to privacy rights that extend far beyond conventional concerns about data security or confidentiality. Privacy, understood as both a fundamental human right and a prerequisite for individual autonomy and dignity, encompasses informational privacy governing personal data, bodily privacy protecting physical integrity, and decisional privacy safeguarding choices about personal matters (Solove, 2008). Biometric systems implicate all three

dimensions simultaneously, capturing bodily information, creating permanent digital records, and influencing individuals' ability to make autonomous choices about identity disclosure and data sharing.

The concept of informational privacy, which protects individuals' ability to control the collection, use, and dissemination of personal information, faces particular strain in biometric contexts where data collection often occurs at points of vulnerability or dependency. Refugees seeking registration for humanitarian assistance, individuals applying for identity documents required for employment or education, or persons crossing borders where biometric verification is mandatory face limited meaningful choice about whether to submit biometric data (Madianou, 2019). This dynamic challenges the foundational data protection principle that processing should be based on freely given, specific, informed consent, as the consequences of refusing biometric enrollment may include exclusion from essential services or legal documentation.

Research conducted in refugee contexts across East Africa has documented patterns where humanitarian organizations and government agencies present biometric enrollment as voluntary while simultaneously making assistance conditional on registration, creating what scholars term "coercive consent" (Hosein & Nyst, 2013). In Kakuma Refugee Camp in Kenya, for example, refugees reported feeling compelled to provide fingerprints and iris scans to access food distributions, despite assurances that participation was voluntary. The practical impossibility of declining enrollment while maintaining access to survival resources undermines the legal fiction of consent as a meaningful protection mechanism. Similar dynamics have been observed in Uganda, Ethiopia, and other contexts where biometric systems mediate access to humanitarian assistance or government services.

Data security represents another critical privacy challenge given the sensitive nature of biometric information and the catastrophic consequences of data breaches or unauthorized access. Unlike passwords or PINs that can be changed if compromised, biometric characteristics are permanent, making breaches potentially irreversible in their impact on individuals' privacy and security. Several African countries have experienced significant data breaches affecting biometric databases, including a 2019 incident in which a vulnerability in a biometric security platform exposed fingerprints and facial recognition data for over one million individuals, including refugees and migrants (Privacy International, 2019). The integration of biometric databases with other government systems and the increasing use of cloud storage create expanded attack surfaces vulnerable to cybercriminals, hostile state actors, or insider threats.

For refugees, the consequences of biometric data breaches extend beyond privacy violations to potential threats to physical safety. Biometric information that identifies refugees from specific ethnic groups, regions, or political affiliations could be exploited by hostile governments or non-state armed groups to locate and target individuals or their family members remaining in countries of origin. Data sharing agreements between host countries and countries of origin, whether formal or informal, create pathways through which biometric

information might flow to actors who pose protection risks. The absence of encryption standards, access controls, and audit mechanisms in many African biometric systems heightens these vulnerabilities (Marwick & boyd, 2018).

Function creep, whereby data collected for one purpose is subsequently used for unrelated purposes without subjects' knowledge or consent, presents a persistent challenge in biometric identity systems across Africa. Biometric databases established ostensibly for civil registration or service delivery purposes are increasingly accessed by law enforcement, intelligence agencies, and immigration authorities for surveillance, investigation, and enforcement activities. Kenya's Integrated Population Registration System, despite being framed as a tool for improving service delivery, has been accessed by security agencies for counterterrorism and crime prevention purposes without clear legal authorization or oversight (Namwaya, 2020). Such function creep directly violates the data protection principle of purpose limitation, which requires that personal information be collected for specified, explicit, and legitimate purposes and not further processed in ways incompatible with those purposes.

The integration of biometric identity systems with emerging technologies including artificial intelligence, facial recognition surveillance networks, and predictive analytics amplifies privacy risks in ways that existing legal frameworks struggle to address. Several African cities have deployed facial recognition systems for public safety and traffic management that could potentially be linked with national biometric identity databases, creating infrastructures of mass surveillance. Rwanda's "Safe City" project, implemented with Chinese technology partners, includes extensive CCTV networks with facial recognition capabilities that could theoretically identify individuals in real-time by matching against biometric identity databases (Mann & Daly, 2019). While governments present these systems as crime prevention tools, civil liberties advocates warn of chilling effects on freedom of assembly, expression, and movement.

For refugee populations who may wish to maintain anonymity to protect themselves from persecution, the integration of facial recognition surveillance with identity databases creates particular hazards. A refugee from Eritrea residing in Ethiopia, for example, might face heightened risks if facial recognition systems operated by Ethiopian authorities could identify their presence and potentially share this information with Eritrean authorities. The principle of confidentiality in refugee status determination, which typically limits sharing of information about asylum seekers or refugees with countries of origin, may be undermined by automated systems that facilitate data sharing or by inadequate controls preventing unauthorized access (Goodwin-Gill & McAdam, 2021).

Algorithmic bias in biometric systems presents another dimension of privacy and rights violations that disproportionately affects African populations and refugees. Research has demonstrated that facial recognition algorithms exhibit significantly higher error rates for individuals with darker skin tones, with some commercial systems showing error rate disparities of more than 100-fold between demographic groups (Buolamwini & Gebru, 2018).

These technical failures can result in false rejections that prevent legitimate access to services, false positives that wrongly implicate individuals in security screenings, and systematic disadvantage for populations already marginalized. When biometric verification systems malfunction due to algorithmic bias, refugees may be denied food assistance, prevented from opening bank accounts, or excluded from education despite having legitimate entitlements.

The opacity of biometric systems and the technical complexity of their operations create substantial barriers to meaningful transparency and accountability. Most refugees and even many government officials lack understanding of how biometric algorithms function, what happens to captured data, who has access to databases, or what safeguards exist against misuse. This information asymmetry undermines individuals' ability to exercise data subject rights such as access, correction, or deletion that legal frameworks may nominally provide (Solove, 2008). When errors occur or data is misused, the pathways for redress remain unclear and often inaccessible, particularly for refugee populations who may lack legal representation or familiarity with administrative complaint mechanisms.

The permanence of biometric data creates temporal dimensions of privacy vulnerability that extend far beyond the immediate context of collection. Biometric information collected from a refugee child during enrollment at age five will remain in databases potentially for decades, yet the child had no capacity to consent to this collection and may have no knowledge of what future uses or risks might emerge. Changes in political circumstances, data governance policies, or technological capabilities could transform benign databases into tools of repression. Historical examples including apartheid-era population registration systems in South Africa demonstrate how identification databases can be weaponized against vulnerable populations when political circumstances change (Breckenridge, 2014).

5. Legal Challenges in Refugee Protection and Biometric Identity

The intersection of refugee protection and biometric identity systems generates distinctive legal challenges that extend beyond general data protection concerns to implicate fundamental principles of asylum law and humanitarian protection. The principle of non-refoulement, considered a cornerstone of international refugee law, prohibits returning refugees to territories where they face threats to life or freedom. This principle extends beyond direct deportation to encompass indirect refoulement through data sharing that exposes refugees to risks in countries of origin or facilitates their identification and apprehension by persecutory actors (Goodwin-Gill & McAdam, 2021). Biometric databases containing refugees' identifying information create potential vectors for violations of non-refoulement when data governance frameworks fail to prevent sharing with hostile governments or actors.

The case of Kenyan government attempts to close Dadaab and Kakuma refugee camps illustrates these dynamics. Proposals for camp closure and forced repatriation of Somali refugees raised concerns that biometric data collected by Kenyan authorities or shared with them by UNHCR could be used to facilitate deportations without adequate protection

screening or could be transferred to Somali authorities in ways that endanger returnees (Human Rights Watch, 2017). Although courts ultimately blocked the closure plans as violating non-refoulement obligations, the incident highlighted vulnerabilities created by extensive biometric databases containing information on refugee populations and the absence of clear legal safeguards preventing data use for deportation purposes.

The legal status ambiguity that characterizes many refugee situations in Africa compounds data protection challenges. Individuals may be registered as asylum seekers awaiting status determination, recognized refugees with formal protection, persons of concern to UNHCR without official refugee status, or undocumented migrants with potential protection needs. Biometric systems often fail to adequately distinguish among these categories, potentially creating risks where data collected in humanitarian contexts might be accessed for immigration enforcement against individuals with legitimate protection claims. Uganda's decision to integrate refugees into its national identification system creates progressive inclusion opportunities but also generates concerns about whether biometric data might be used to enforce mobility restrictions or deportations if policies shift (Omata, 2020).

The voluntary nature of repatriation, a fundamental principle of refugee protection, requires that decisions to return to countries of origin be made freely without coercion. However, biometric systems that condition access to assistance on enrollment or that track refugees' movements and behavior create surveillance infrastructures that could be used to pressure refugees toward repatriation. Ethiopia's implementation of the Comprehensive Refugee Response Framework included biometric registration that tracked refugees' economic activities and social connections, raising concerns that this information might inform decisions to reduce assistance or encourage returns irrespective of whether conditions in Eritrea or South Sudan supported voluntary repatriation (Bilak & Caterina, 2018).

The right to asylum, recognized in the Universal Declaration of Human Rights and regional frameworks including the African Charter on Human and Peoples' Rights, encompasses procedural protections including the right to have protection claims fairly assessed and the right to remain in a country of refuge pending status determination. Biometric systems deployed at borders or in immigration enforcement contexts may interfere with these rights when they facilitate rapid deportations without adequate screening or when they create barriers to accessing asylum procedures. Several North African countries have implemented biometric systems at borders that European Union agencies access for migration control purposes, potentially enabling returns of individuals with protection needs before they can access asylum procedures (Mixed Migration Centre, 2021).

Legal identity rights, increasingly framed as fundamental human rights essential for accessing other rights and services, present particular challenges for refugee populations who may lack birth certificates or other conventional identity documentation. The UN Sustainable Development Goal 16.9 calls for legal identity for all by 2030, and biometric systems are often presented as solutions for providing identity to populations that governments consider "invisible" (Breckenridge, 2014). For refugees, however, the relationship between biometric

identity and legal recognition is complex and potentially contradictory. While biometric registration might provide refugees with identity credentials that facilitate access to services, these same credentials may reinforce their status as non-citizens and create permanent digital markers of their refugee identity that could generate discrimination or exclusion.

Somalia's biometric voter registration system exemplifies these tensions. Designed to enhance electoral integrity by ensuring voters could only cast ballots once and to facilitate democratic participation, the system inadvertently created barriers for Somali refugees residing in Kenya, Uganda, and other neighboring countries who held Somali citizenship but lacked access to enrollment centers. The technical decision to require in-person biometric enrollment effectively disenfranchised portions of the diaspora, raising questions about whether identity systems enhance or undermine fundamental rights (Human Rights Watch, 2021). Similar dynamics emerge in contexts where refugees hold citizenship in countries of origin but cannot safely return to complete biometric enrollment for national identity documents or passports.

The principle of family unity, recognized in refugee law as requiring that families not be separated through protection processes and that opportunities exist for family reunification, intersects problematically with biometric identity systems. Family relationship verification increasingly depends on biometric links established through DNA testing or shared biographical databases, yet many refugee families lack documentation proving relationships due to displacement circumstances. Ethiopia's biometric registration of Eritrean refugees has revealed challenges where family members separated during flight from persecution have difficulty reunifying if biometric enrollment occurred separately and biographical information does not establish connections (Bilak & Caterina, 2018). The prioritization of biometric verification over other forms of relationship evidence can effectively separate family members with legitimate relationships simply because they lack biometric enrollment that algorithmically links them.

Children's rights present particularly acute legal challenges in refugee contexts with biometric systems. The Convention on the Rights of the Child, ratified by every African country, recognizes children's rights to privacy, protection from exploitation, and consideration of their best interests in decisions affecting them. Biometric enrollment of refugee children raises questions about consent capacity, given that parents or guardians typically provide consent on behalf of children but may themselves lack adequate information about data processing practices or long-term implications. The permanence of biometric data means that decisions made by or for children at young ages will affect their privacy and identity for decades, yet legal frameworks rarely establish enhanced protections for children's biometric information (Livingstone, 2018).

UNHCR's policy framework for biometric data protection, revised in 2018, establishes standards for the organization's own biometric operations but faces implementation challenges and does not bind host country governments or partner organizations that may access or share refugee data. The policy recognizes principles including lawfulness, fairness,

transparency, purpose limitation, data minimization, accuracy, storage limitation, security, and accountability, aligning generally with international data protection standards. However, the policy contains broad exceptions permitting data sharing for purposes including resettlement, investigation of fraud, and protection verification, raising concerns about circumstances under which refugee data might be disclosed (UNHCR, 2018). The absence of independent oversight mechanisms or accessible complaint procedures for refugees who believe their data has been mishandled limits the practical enforceability of these policy commitments.

The legal doctrine of humanitarian exception, which permits processing of personal data without consent in contexts of humanitarian emergency or where vital interests of data subjects are at stake, has been invoked to justify biometric enrollment of refugees. However, critics argue that this exception is applied too broadly to situations that do not meet the stringent requirements for overriding consent principles, and that alternatives such as anonymous assistance distribution or paper-based registration could achieve humanitarian objectives without creating expansive biometric databases (Madianou, 2019). The question of whether biometric enrollment genuinely serves refugees' vital interests or primarily serves organizational efficiency and fraud prevention objectives remains contested and underexamined in legal frameworks.

6. Case Studies: Biometric Identity Implementation and Refugee Protection Across Africa

Examining specific national and regional implementations of biometric identity systems reveals the concrete manifestations of legal challenges and their impacts on refugee populations across diverse African contexts. Kenya's approach to refugee documentation and biometric enrollment exemplifies tensions between security imperatives, humanitarian protection, and privacy rights. The country hosts approximately 600,000 refugees primarily from Somalia, South Sudan, Democratic Republic of Congo, and Ethiopia, with populations concentrated in Dadaab and Kakuma camps as well as urban areas particularly Nairobi (UNHCR, 2023).

Kenya's refugee management framework mandates biometric registration through the Refugee Affairs Secretariat, creating databases distinct from the national Huduma Namba system from which refugees are explicitly excluded. This dual documentation approach reflects Kenya's encampment policy and its treatment of refugees as temporary populations whose integration should be limited. Refugees receive Alien Cards following biometric enrollment, which serve as both identity documents and movement passes restricting them to designated areas. The biometric registration process captures fingerprints, photographs, and iris scans, linking this information to demographic data and assigned refugee numbers (Namwaya, 2020). However, the legal framework governing this data collection, storage, sharing, and security remained unclear until Kenya's 2019 Data Protection Act, and implementation of that Act's provisions to existing refugee biometric databases has been inconsistent.

UNHCR operates parallel biometric registration through its BIMS system in Kenya, creating a situation where refugees are enrolled in multiple overlapping databases controlled by different entities with varying data governance standards. Tensions between UNHCR and Kenyan authorities regarding data sharing have emerged periodically, particularly when the government has sought access to UNHCR's biometric databases to support security operations or enforcement activities. UNHCR's policy framework limits data sharing to purposes aligned with protection, but the organization's dependence on host government cooperation and the absence of clear legal protocols governing such requests create vulnerabilities (Jacobsen, 2015). In 2019, Kenyan security agencies reportedly obtained access to biometric data on Somali refugees during counterterrorism operations, raising concerns about profiling and collective punishment of refugee communities based on ethnic or national origin associations with security threats.

The Nubian Rights Forum litigation challenging Kenya's Huduma Namba system provides important judicial precedent regarding biometric data protection requirements. The High Court's 2020 ruling found that the national identification system lacked adequate legal framework, had not conducted proper privacy impact assessments, failed to establish clear data protection safeguards, and did not provide sufficient transparency about data sharing arrangements (Nubian Rights Forum & Others v Attorney General & 6 Others, 2020). The court suspended full implementation pending establishment of proper protections, establishing principles that should apply equally to refugee biometric systems though application to that context remains uncertain. The judgment recognized that biometric data implicated constitutional privacy rights under Article 31 of Kenya's Constitution and that state collection of such information required robust legal authorization and safeguards proportionate to privacy intrusions.

Uganda's refugee management approach contrasts sharply with Kenya's encampment model, offering one of Africa's most progressive legal frameworks through its 2006 Refugees Act and subsequent amendments. Uganda hosts over 1.5 million refugees, making it one of the world's largest refugee-hosting countries, with populations primarily from South Sudan, Democratic Republic of Congo, Burundi, and Somalia (UNHCR, 2023). Ugandan law provides refugees with freedom of movement, the right to work, access to education and healthcare, and importantly for digital identity purposes, the possibility of inclusion in national identification systems including biometric enrollment for national IDs.

The National Identification and Registration Authority (NIRA) in Uganda has progressively enrolled refugees in the national biometric identity system, issuing national ID cards that enable refugees to open bank accounts, register businesses, acquire mobile phone SIM cards, and access government services on par with citizens in many respects. This inclusive approach reflects Uganda's broader refugee policy framework and its implementation of the Comprehensive Refugee Response Framework piloted in the country (Omata, 2020). However, the integration of refugees into national biometric systems creates questions about data governance and protection that Uganda's 2019 Data Protection and Privacy Act addresses only partially. Concerns persist about whether refugee biometric data might be

shared with countries of origin, accessed for security operations that disproportionately target refugee communities, or used to enforce restrictions on movement despite legal provisions for mobility.

The Bidibidi refugee settlement in northern Uganda, established in 2016 following South Sudanese displacement, became a testing ground for biometric identity systems operated by multiple actors including UNHCR, the World Food Programme, the Ugandan government, and various NGOs providing services. Refugees in Bidibidi underwent biometric enrollment at multiple points including initial registration upon arrival, verification for food assistance distribution, enrollment in livelihood programs, and national ID registration (Omata, 2020). This proliferation of biometric data collection raised concerns about coordination, interoperability, consent processes, and refugees' understanding of what data was being collected and for what purposes. Research conducted with refugees in the settlement revealed limited awareness of data protection rights, confusion about relationships among different biometric systems, and concerns about potential data sharing with South Sudanese authorities.

South Africa's refugee protection framework operates within the context of one of Africa's most developed biometric identity infrastructures and comprehensive data protection legislation. The country hosts approximately 260,000 refugees and asylum seekers, though irregular migration flows complicate precise enumeration (UNHCR, 2023). South Africa's Department of Home Affairs maintains biometric databases that include both citizens and documented foreign nationals including recognized refugees who receive refugee identity documents with fingerprint biometrics. The Refugees Act of 1998 provides for asylum seekers to receive permits while their applications are adjudicated, and refugees who receive positive determinations obtain identity documents that should facilitate integration.

However, implementation challenges have plagued South Africa's refugee documentation system, with extensive backlogs in asylum processing, limited issuance of refugee IDs, and administrative obstacles preventing many recognized refugees from obtaining the identity documents to which they are legally entitled. Civil society organizations have documented cases where refugees' biometric data was captured during asylum application but documentation was never issued or renewals were denied without explanation (Amit & Kriger, 2014). The absence of valid identity documents despite having been biometrically enrolled creates paradoxical situations where refugees exist in databases yet cannot access services or exercise rights that depend on presenting physical documentation. This disconnect between biometric enrollment and document issuance illustrates that technological systems alone cannot guarantee legal recognition or rights realization without functional administrative processes.

South Africa's deployment of biometric systems at ports of entry and its maintenance of a Movement Control System that tracks foreign nationals' entry, stay, and exit creates extensive surveillance of non-citizens including refugees. The Protection of Personal Information Act should govern this data processing, but enforcement has been limited and foreign nationals

face particular vulnerabilities given weaker legal standing to challenge government data practices (Roos, 2021). Concerns have emerged about data sharing between South African authorities and countries of origin in contexts where such sharing could compromise refugee protection, particularly regarding Zimbabwean asylum seekers whose biometric information might be accessible to Zimbabwean authorities through bilateral security cooperation agreements.

Ethiopia's implementation of biometric identity systems for refugees occurs in a context where the country hosts over 1 million refugees primarily from Eritrea, South Sudan, Somalia, and Sudan, making it one of Africa's largest refugee-hosting nations (UNHCR, 2023). Ethiopia's 2019 Refugee Proclamation represents significant reform aligning the legal framework with international standards and facilitating greater refugee integration including access to work permits and national identification systems. However, implementation has been uneven and affected by political instability including the Tigray conflict and tensions with Eritrea that directly affect refugee populations.

The Ethiopian government operates the Refugees and Returnees Service alongside UNHCR to manage refugee registration and documentation, with biometric enrollment conducted at reception centers and refugee camps. Ethiopian authorities have increasingly sought integration of refugee biometric data with national identity systems as part of implementing the 2019 Proclamation's progressive provisions. However, concerns persist particularly regarding Eritrean refugees whose biometric information could theoretically be accessed by Eritrean authorities given complex bilateral relations between the two countries (Bilak & Caterina, 2018). Ethiopia's 2021 Data Protection Proclamation establishes a framework for personal data protection including requirements for consent, purpose limitation, and security measures, though specific application to refugee contexts and enforcement capacity remain uncertain.

The situation of Eritrean refugees in Ethiopia highlights particular vulnerabilities at the intersection of biometric identity and protection. Following the 2018 peace agreement between Ethiopia and Eritrea, border openings and increased diplomatic cooperation raised concerns about whether refugee data might be shared between the countries despite protection obligations. Reports emerged of Eritrean refugees being pressured to return or facing surveillance by Eritrean agents operating in Ethiopia, raising questions about whether biometric databases might facilitate such activities (Human Rights Watch, 2021). The principle of confidentiality regarding refugee identity becomes particularly critical in contexts where countries of origin and asylum maintain diplomatic relations and security cooperation that could create pathways for data sharing.

Tanzania's management of Burundian refugee populations illustrates challenges in balancing encampment policies, repatriation promotion, and biometric identity systems. Tanzania hosts over 240,000 refugees primarily from Burundi and Democratic Republic of Congo in camps in western Tanzania (UNHCR, 2023). The government's citizenship pathway for long-settled Burundian refugees who arrived in 1972 included biometric enrollment and verification

processes intended to distinguish those eligible for naturalization from more recent arrivals. This biometric sorting process created contentious situations where family members might be separated based on biometric enrollment timing or where individuals' eligibility depended on algorithmic matching against historical records.

Tanzania's promotion of voluntary repatriation for post-2015 Burundian refugees has involved use of biometric systems to document returns and prevent multiple assistance claims. However, concerns have been raised about whether repatriation decisions were genuinely voluntary given pressures applied to refugees including assistance reductions, movement restrictions, and administrative obstacles to obtaining documentation (Human Rights Watch, 2018). The role of biometric systems in facilitating returns that may not meet voluntary repatriation standards illustrates how digital identity infrastructure can become implicated in protection violations rather than supporting protection objectives.

Regional initiatives including the East African Community's integrated border management systems incorporate biometric components intended to facilitate regional mobility while enhancing security. However, these systems create questions about data governance particularly regarding refugee populations who may move across borders within the region. A Congolese refugee who initially sought asylum in Uganda but subsequently moved to Kenya would potentially be biometrically enrolled in multiple national systems, with unclear protocols governing how this information might be shared across borders or accessed by authorities in different countries. The absence of harmonized data protection standards and mutual recognition agreements creates regulatory gaps where refugees' information may flow across borders without adequate safeguards.

The case of South Sudanese refugees dispersed across multiple neighboring countries including Uganda, Kenya, Ethiopia, and Sudan illustrates challenges in coordinating biometric identity systems across jurisdictions. Family members separated during displacement might be registered in different countries' refugee databases with limited mechanisms for linking records or facilitating family reunification across borders. UNHCR's regional information management systems aim to address these challenges, but interoperability limitations and data sovereignty concerns complicate cross-border data sharing even for protection purposes (UNHCR, 2022). The technical architecture of biometric systems designed primarily for national contexts struggles to accommodate the transnational nature of refugee movements and the need for coordinated regional responses.

7. Stakeholder Perspectives and Governance Challenges

The implementation and governance of biometric identity systems for refugees involve multiple stakeholders with divergent interests, priorities, and perspectives that create complex dynamics shaping policy and practice. Host governments prioritize security concerns, administrative efficiency, and domestic political considerations that may not always align with refugee protection principles or privacy rights. Security agencies view biometric databases as valuable tools for counterterrorism, crime prevention, and border control, often pressing for expanded access to refugee biometric data despite protection concerns

(Madianou, 2019). Political pressures to demonstrate control over refugee populations and to respond to public concerns about security or resource competition can drive expansion of surveillance systems without adequate attention to rights implications.

Administrative efficiency motivations drive many governments' enthusiasm for biometric identity systems, with promises that digital identification will streamline service delivery, reduce fraud, and improve resource allocation. Kenya's Huduma Namba system exemplifies this efficiency rationale, promoted as a means to consolidate multiple identity documents, facilitate access to government services, and enhance coordination across agencies (Namwaya, 2020). For refugee administration specifically, governments and humanitarian organizations argue that biometric enrollment prevents individuals from registering multiple times to access assistance fraudulently, ensures equitable distribution of resources, and creates accountability mechanisms. However, these efficiency gains must be weighed against privacy costs and risks of exclusion when systems malfunction or when emphasis on fraud prevention creates barriers to legitimate assistance access.

International organizations, particularly UNHCR and the World Food Programme, operate as both advocates for refugee protection and implementers of biometric systems, creating potential tensions between these roles. UNHCR's deployment of biometric identity management systems across refugee contexts globally reflects the organization's perspective that digital identity serves protection objectives by establishing refugees' identity, preventing trafficking and exploitation of children, supporting family reunification, and facilitating resettlement processes (UNHCR, 2018). The organization presents biometric enrollment as enabling more effective protection interventions and ensuring assistance reaches intended beneficiaries rather than being diverted through fraud.

However, UNHCR's position as both data controller for biometric systems and protection mandate holder creates inherent conflicts of interest that critics argue compromise independent protection assessment. When the same organization collecting biometric data also determines protection needs and distributes assistance, refugees face limited ability to decline enrollment without risking their access to protection services (Jacobsen, 2015). UNHCR's dependence on host government cooperation and its need to maintain working relationships with national authorities can constrain its advocacy on data protection issues, particularly when governments seek access to refugee biometric data for purposes that may not align with protection principles. The organization's lack of independence from donor government priorities, many of which emphasize migration control and border security, further complicates its positioning on biometric identity governance.

Non-governmental organizations providing services to refugees face complex decisions about whether to implement their own biometric systems or rely on UNHCR and government databases for beneficiary identification. Some organizations have developed independent biometric enrollment for specific programs such as education, healthcare, or livelihood support, contributing to the proliferation of parallel systems and repeated biometric capture from refugee populations. Other NGOs have resisted implementing biometric systems due to

privacy concerns, recognition of power imbalances inherent in requiring vulnerable populations to submit biometric data, or practical concerns about cost and technical capacity (Madianou, 2019). These decisions reflect underlying tensions in humanitarian principles including respect for human dignity, autonomy, and the "do no harm" principle that requires careful consideration of whether technological interventions might create risks that outweigh benefits.

Civil society organizations focused on digital rights, privacy, and refugee advocacy have emerged as critical voices challenging biometric system deployments that lack adequate safeguards. Organizations including Privacy International, Access Now, the Refugee Law Project, and various national human rights organizations have documented risks associated with biometric refugee databases, advocated for stronger legal protections, and supported litigation challenging privacy violations (Privacy International, 2019). These advocacy efforts have achieved some successes including court decisions requiring privacy impact assessments, regulatory actions addressing inadequate data protection, and policy reforms strengthening safeguards. However, civil society capacity remains limited relative to the scale of biometric system deployment, and refugee populations themselves often lack representation in policy discussions about digital identity governance.

Private sector technology providers play significant though often opaque roles in developing and operating biometric systems deployed in refugee contexts. Companies including Idemia, Thales, and various national technology firms contract with governments and international organizations to provide biometric hardware, software, databases, and technical support. These commercial relationships create questions about data access, security standards, and corporate accountability that existing legal frameworks address inadequately (Mann & Daly, 2019). Terms of service, data processing agreements, and intellectual property arrangements governing these commercial relationships are typically not public, limiting transparency about corporate actors' roles in refugee data governance.

The involvement of technology companies from countries including France, China, and the United States in African biometric systems creates additional sovereignty and geopolitical dimensions. Concerns have been raised about whether foreign companies or governments might access biometric data collected in African contexts, whether through backdoors in technical systems, cloud storage in foreign jurisdictions, or intelligence sharing agreements (Feldstein, 2019). For refugee populations from countries experiencing conflicts with geopolitical dimensions, the nationality and affiliations of technology providers may have protection implications that are rarely considered in procurement or deployment decisions.

Refugees themselves, as the populations most directly affected by biometric identity systems, often have limited voice in governance decisions despite principles of participation and consultation that should inform humanitarian interventions. Research documenting refugees' perspectives on biometric systems reveals complex and nuanced views rather than uniform opposition or acceptance. Some refugees view biometric identity documents as valuable tools that facilitate access to services, provide official recognition, and may support integration or

resettlement (Omata, 2020). Others express concerns about privacy violations, fears of data sharing with countries of origin, discomfort with bodily data capture, and distrust of authorities collecting information without clear explanation of purposes or protections.

Language barriers, power imbalances, and limited understanding of technical systems constrain meaningful consent and participation in biometric governance for many refugees. Information provided during enrollment is often minimal, presented in languages refugees may not fully understand, and fails to adequately explain data processing practices, storage duration, sharing arrangements, or security measures (Jacobsen, 2015). The absence of accessible complaint mechanisms or data subject rights enforcement procedures leaves refugees with little recourse when problems arise including enrollment errors, assistance denials due to system malfunctions, or suspected data misuse. This lack of accountability and redress compounds the power asymmetries inherent in contexts where already vulnerable populations must submit to biometric capture to access survival resources.

Gender dimensions of biometric identity systems create specific concerns particularly for refugee women and girls who may face heightened risks from data exposure. Women fleeing gender-based violence or forced marriage may require anonymity to protect their safety, yet biometric systems create permanent digital records that could potentially be accessed by abusers, family members, or community actors seeking to locate them (UN Women, 2018). Cultural and religious considerations affect some women's comfort with biometric capture procedures particularly when enrollment requires physical contact with technology operators or uncovering of faces or hands in contexts where gender segregation or covering norms are significant. The design of biometric systems rarely incorporates adequate attention to these gendered dimensions, with enrollment procedures, operator training, and data protection measures often failing to address specific vulnerabilities that women and girls face.

Children's perspectives on biometric enrollment remain particularly underexplored despite their significant presence in refugee populations and their particular vulnerabilities. Children lack capacity to provide informed consent to biometric capture, yet decisions made by parents, guardians, or authorities on their behalf will affect their privacy and identity for decades. The absence of age-appropriate information, consent procedures designed for children, or special protections for children's biometric data reflects broader patterns where children's rights receive inadequate attention in digital identity governance (Livingstone, 2018). As children enrolled in biometric systems during refugee contexts grow to adulthood, questions emerge about their ability to understand, challenge, or seek deletion of data captured when they were too young to consent, particularly when political or security circumstances change.

8. Comparative Legal Analysis and International Standards

Examining biometric identity governance in Africa against international and comparative legal standards reveals substantial gaps between existing African frameworks and more comprehensive protections established in other jurisdictions. The European Union's General Data Protection Regulation (GDPR), which entered into force in 2018, establishes the most

comprehensive framework globally for biometric data protection. The GDPR classifies biometric data processed for unique identification purposes as a special category of personal data subject to heightened protections under Article 9, prohibiting processing except under specific limited circumstances including explicit consent, substantial public interest with appropriate safeguards, or vital interest protection (Voigt & Von dem Bussche, 2017).

The GDPR's principles including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability provide a comprehensive framework that most African data protection laws aspire toward but implement less rigorously. Particularly significant is the GDPR's requirement for data protection impact assessments before implementing systems that pose high risks to individuals' rights and freedoms, including biometric processing. This requirement mandates that organizations systematically identify and mitigate privacy risks before deployment rather than addressing problems after systems are operational. Few African countries have implemented comparable impact assessment requirements, and where such provisions exist, enforcement and public transparency remain limited (Greenleaf, 2020).

The GDPR's robust enforcement mechanisms including substantial financial penalties, independent supervisory authorities with investigative powers, and data subjects' rights to judicial remedies create accountability structures largely absent in African contexts. Maximum fines reaching 4% of global annual revenue or €20 million provide meaningful deterrence for organizations contemplating privacy violations. In contrast, most African data protection frameworks include nominal penalties that provide insufficient incentive for compliance, and data protection authorities often lack resources, independence, or political support necessary for effective enforcement (Roos, 2021).

The extraterritorial application of the GDPR affects African biometric systems when personal data of EU residents is processed or when organizations established in Africa offer services to individuals in the EU. European humanitarian organizations and technology companies operating in African refugee contexts must ensure their data processing complies with GDPR standards, potentially creating situations where refugees in Africa receive greater data protections through European organizations than they would from host governments or non-European actors. This regulatory patchwork creates inequities where protection depends on which organizations collect and control biometric data rather than on uniform standards applied consistently.

The United Nations' Principles and Guidelines on Privacy and Data Protection provide international standards developed by the UN Human Rights Council that should inform biometric system governance globally. These principles establish that privacy is a fundamental human right integral to human dignity and freedom, that data protection measures should safeguard individuals against arbitrary or unlawful interference with privacy, and that personal data processing should respect principles including lawfulness, fairness, purpose specification, data minimization, and security (Office of the United Nations High Commissioner for Human Rights, 2018). The principles emphasize that special

protection should apply to particularly sensitive information including data revealing racial or ethnic origin, political opinions, or religious beliefs, categories particularly relevant to refugee contexts where such information may relate to persecution grounds.

The UN Human Rights Committee's General Comment No. 16 on Article 17 of the International Covenant on Civil and Political Rights establishes that the right to privacy encompasses protection against surveillance and data collection by both state and private actors. The Committee has emphasized that technological developments require strengthening privacy protections and that states have obligations to prevent interference with privacy through legal frameworks, oversight mechanisms, and remedies for violations (United Nations Human Rights Committee, 1988). These standards apply to biometric systems deployed in Africa regardless of whether domestic legislation incorporates them, creating international legal obligations that can be invoked to challenge inadequate data protection.

The UN Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, establish that businesses including technology companies providing biometric systems have responsibilities to respect human rights including privacy. The principles require human rights due diligence through which companies identify, prevent, mitigate, and account for adverse human rights impacts of their products and services (Ruggie, 2011). This framework should apply to private sector actors providing biometric identity systems in refugee contexts, requiring that they assess whether their technologies might facilitate privacy violations, surveillance abuses, or protection violations and that they implement mitigation measures including declining contracts where adequate safeguards cannot be ensured.

However, implementation of corporate human rights responsibilities in African biometric contexts remains minimal, with limited evidence that technology providers conduct meaningful human rights impact assessments or decline projects that pose unacceptable risks. The absence of mandatory human rights due diligence requirements in most national legal frameworks and weak enforcement of existing principles allows commercial interests to proceed without adequate attention to rights implications. Civil society efforts to hold companies accountable through naming and shaming, shareholder advocacy, or strategic litigation have achieved limited success given the opacity of commercial relationships and the complexity of tracing responsibility for harms through supply chains and contractual arrangements (Privacy International, 2019).

India's Aadhaar biometric identity system, which has enrolled over 1.3 billion residents, provides a comparative example of large-scale biometric implementation accompanied by significant legal challenges and privacy concerns. The Indian Supreme Court's 2018 judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India recognized privacy as a fundamental right under the Indian Constitution and imposed significant restrictions on Aadhaar including prohibiting mandatory linkage for private sector services and requiring stronger data protection safeguards (Supreme Court of India, 2018). While the judgment

upheld Aadhaar's validity for government welfare programs with appropriate limitations, it established principles relevant globally including that biometric systems must be necessary and proportionate, that alternatives should be available for individuals unable or unwilling to provide biometric data, and that robust data protection frameworks must accompany digital identity deployment.

The Aadhaar litigation revealed problems common to large-scale biometric systems including enrollment errors excluding eligible individuals, authentication failures preventing service access, data breaches exposing personal information, and function creep whereby systems established for limited purposes expanded to encompass broader surveillance and social control (Khera, 2019). These challenges documented in the Indian context find parallels in African biometric implementations, suggesting that technical and governance problems are not context-specific but rather inherent to biometric identity systems absent robust legal protections and accountability mechanisms.

Estonia's digital identity system offers a contrasting model emphasizing strong data protection, user control, and decentralized architecture. Estonian residents receive digital identity cards enabling electronic authentication and digital signatures, with cryptographic protections and audit trails documenting every instance of access to personal information. Citizens can monitor who has accessed their data and for what purposes through transparent logging systems, and strict limitations constrain data sharing across government agencies (Anthes, 2015). While Estonia's context differs substantially from African refugee settings, the emphasis on transparency, user control, and minimal data collection provides principles applicable to protecting vulnerable populations' digital identity.

The Council of Europe's Convention 108+ on data protection, updated in 2018, establishes international standards for the protection of individuals with regard to automatic processing of personal data. The Convention recognizes biometric data as sensitive requiring heightened protection and establishes principles including legitimate and specified purposes, data quality and proportionality, special protections for sensitive data, data security, transparency, and data subjects' rights including access, correction, and complaint (Council of Europe, 2018). The Convention is open to accession by non-European countries, offering a pathway for African states to align their frameworks with international standards and benefit from regional cooperation on data protection governance.

9. Recommendations for Legal Reform and Rights Protection

Addressing the legal challenges at the intersection of biometric identity, privacy rights, and refugee protection requires comprehensive reforms spanning national legislation, regional frameworks, international standards, and operational practices. This section proposes specific recommendations directed at governments, international organizations, civil society, and private sector actors responsible for implementing and governing biometric systems affecting refugee populations.

9.1 Strengthening National Data Protection Frameworks

African governments should prioritize enactment and implementation of comprehensive data protection legislation that explicitly addresses biometric information as a special category requiring heightened safeguards. Legislation should establish clear legal bases for biometric data processing, with explicit consent as the primary basis supplemented by narrowly defined exceptions for contexts where consent is genuinely impossible or inappropriate (Greenleaf, 2020). For refugee populations, legal frameworks must recognize power imbalances and dependencies that compromise meaningful consent, requiring additional safeguards including independent oversight, rights-respecting alternatives to biometric systems, and enhanced transparency about data processing practices.

Data protection legislation should mandate privacy impact assessments before deploying biometric systems, with assessments conducted by independent evaluators and made publicly available to enable scrutiny by civil society and affected communities. Impact assessments should specifically analyze risks to vulnerable populations including refugees, evaluate alternatives that might achieve objectives with less privacy intrusion, and propose mitigation measures addressing identified risks. Kenya's High Court ruling requiring privacy impact assessment for the Huduma Namba system provides a judicial precedent that should be codified in legislation and extended to all biometric systems including those targeting refugee populations (Nubian Rights Forum & Others v Attorney General & 6 Others, 2020).

Legislation must establish independent data protection authorities with adequate resources, technical expertise, and political independence necessary for effective oversight and enforcement. These authorities should possess investigative powers enabling them to examine biometric systems' compliance with legal requirements, order corrective measures when violations are identified, and impose meaningful penalties deterring non-compliance. Data protection authorities should proactively engage with refugee populations and organizations representing their interests, ensuring that oversight reflects the specific vulnerabilities and concerns of displaced populations (Roos, 2021).

Legal frameworks should guarantee data subjects' rights including access to their personal information, correction of inaccuracies, erasure when data is no longer necessary for its original purpose, and objection to processing in circumstances where privacy interests outweigh processing purposes. For refugees, exercising these rights requires accessible mechanisms that accommodate language diversity, recognize limited digital literacy, and provide support navigating administrative procedures. Legislation should establish obligations for data controllers to provide information in languages refugees understand and to create accessible complaint mechanisms that do not require legal representation or impose cost barriers.

9.2 Harmonizing Regional Data Protection Standards

The African Union should prioritize achieving ratifications necessary for the Malabo Convention to enter into force, creating a foundation for regional harmonization of data

protection standards. The Convention should be supplemented with detailed guidelines specifically addressing biometric systems and refugee protection, filling current gaps regarding special safeguards for vulnerable populations. Regional economic communities including ECOWAS, EAC, and SADC should adopt and implement supplementary data protection frameworks establishing minimum standards for member states and facilitating cross-border data protection cooperation (African Union, 2014).

Regional frameworks should establish mechanisms for coordinating data protection oversight across borders, enabling data protection authorities in different countries to cooperate on investigations involving cross-border data flows or regional biometric systems. Mutual recognition agreements should facilitate enforcement of data protection decisions across jurisdictions, preventing organizations from evading accountability by locating operations in countries with weaker enforcement. Regional cooperation mechanisms should specifically address refugee contexts where individuals may move across borders and be enrolled in multiple national systems, establishing protocols for protecting refugees' data throughout their displacement journeys.

The African Commission on Human and Peoples' Rights should develop comprehensive guidance on the application of the African Charter's privacy protections to biometric identity systems, establishing regional human rights standards that states must respect. The Commission should use its complaint mechanisms to address cases where biometric systems violate refugees' rights, developing jurisprudence that interprets privacy and data protection obligations in light of technological developments. Regional human rights mechanisms can complement data protection authorities' technical oversight by emphasizing the human rights dimensions of digital identity governance and holding states accountable for violations affecting refugee populations (Manby, 2016).

9.3 Integrating Data Protection with Refugee Protection Frameworks

International refugee law frameworks including the 1951 Refugee Convention, the OAU Refugee Convention, and national refugee legislation should be explicitly harmonized with data protection requirements. Legislative reforms should recognize that the principle of confidentiality in refugee status determination extends to biometric data, prohibiting sharing of refugees' biometric information with countries of origin or other actors who might pose protection risks. Legal frameworks should establish clear protocols for evaluating data sharing requests, requiring protection assessments before any transfer and empowering refugees to challenge sharing decisions affecting their safety (Goodwin-Gill & McAdam, 2021).

Refugee legislation should guarantee that identity documentation, including biometric enrollment, cannot be made a prerequisite for accessing asylum procedures or fundamental protection. While biometric systems may facilitate certain administrative processes, individuals unable or unwilling to provide biometric data must have alternative pathways for establishing identity and accessing protection. Particular accommodation should be made for

individuals whose biometric characteristics are affected by torture, medical conditions, or other circumstances, ensuring that technical limitations do not result in protection denials.

UNHCR should strengthen its data protection policy framework to incorporate more robust safeguards, clearer limitations on data sharing, and enhanced accountability mechanisms. The organization should establish an independent data protection oversight body with authority to investigate complaints, audit biometric systems, and require corrective measures when violations occur. Refugees should have access to transparent complaint processes that provide meaningful remedies including data deletion, compensation for harms, and changes to policies or practices that violate privacy rights (UNHCR, 2018).

9.4 Ensuring Meaningful Consent and Participation

Operational procedures for biometric enrollment should be reformed to ensure truly informed and voluntary consent, particularly in refugee contexts. Information provided to refugees during enrollment must comprehensively explain what biometric data is being collected, how it will be stored, who will have access, for what purposes it may be used, how long it will be retained, and what rights refugees have regarding their data. This information must be provided in languages refugees understand, using plain language accessible to individuals without technical backgrounds, and allowing adequate time for questions and reflection before enrollment occurs (Jacobsen, 2015).

Consent processes should be documented in ways that demonstrate refugees' understanding and voluntary agreement, moving beyond checkbox consent forms to interactive processes that verify comprehension. Refugees should explicitly affirm that they understand they are providing consent freely, that they comprehend the implications of biometric enrollment, and that they know they can withdraw consent for certain uses of their data subject to limitations necessary for protection purposes. Documentation should specify the particular purposes for which consent is provided, enabling refugees to consent to some uses while declining others.

Participation mechanisms should be established enabling refugees to meaningfully influence biometric system governance decisions affecting them. Refugee representatives should be included in advisory boards overseeing biometric systems, in privacy impact assessment processes, and in policy development regarding data protection standards. Organizations implementing biometric systems should conduct regular consultations with refugee communities, creating feedback loops through which concerns can be raised and addressed. Governance structures should move beyond tokenistic consultation toward genuine power-sharing that gives refugees voice in decisions affecting their privacy and dignity (Madianou, 2019).

9.5 Implementing Technical Safeguards and Security Standards

Technical architecture of biometric systems must incorporate privacy-by-design principles, implementing safeguards at the system design stage rather than attempting to retrofit protections after deployment. Data minimization should guide system design, with collection

limited to information genuinely necessary for specified purposes and with regular review of whether collected data remains necessary. Biometric databases should implement strict access controls limiting who can query databases, for what purposes, and with robust audit trails documenting every access instance (Cavoukian, 2009).

Encryption should be mandatory for biometric data both in storage and transmission, using strong cryptographic standards that protect information from unauthorized access. Biometric templates should be stored using irreversible transformation algorithms that enable identity verification without retaining raw biometric images, reducing risks in the event of database breaches. Systems should implement multi-factor authentication and privileged access management ensuring that database access requires multiple credentials and that the number of individuals with administrative access is minimized.

Regular security audits should be conducted by independent evaluators assessing vulnerabilities and compliance with security standards. Audit results should be made public in appropriately redacted form, enabling external scrutiny of security claims while protecting specific technical details that might facilitate attacks. Incident response plans should be established detailing procedures to follow when breaches occur, including notification obligations to affected individuals, data protection authorities, and relevant protection actors when refugees' data is compromised (Privacy International, 2019).

9.6 Establishing Corporate Accountability Mechanisms

Private sector technology providers should be subject to mandatory human rights due diligence requirements, compelling them to assess and address privacy and protection risks before providing biometric systems in refugee contexts. Procurement processes should require that vendors demonstrate compliance with international data protection and human rights standards, including GDPR-equivalent protections regardless of jurisdiction. Contracts should include explicit data protection obligations, prohibitions on data sharing beyond specified purposes, and remedies including contract termination when vendors fail to maintain adequate safeguards (Ruggie, 2011).

Technology companies should be required to conduct algorithmic impact assessments evaluating whether their biometric systems exhibit bias disadvantaging particular demographic groups including refugees from specific regions or ethnic backgrounds. Assessment results should be publicly disclosed and systems demonstrating unacceptable accuracy disparities should not be deployed until bias is remedied. Ongoing monitoring should track system performance across demographic groups, identifying and addressing accuracy problems that emerge during operation.

Corporate transparency should be enhanced through requirements that companies publicly disclose which governments and organizations they supply biometric systems to, general categories of data processing involved, and aggregate information about system scale and performance. Transparency reports should include information about government or organizational requests for data access, the legal bases for such requests, and the frequency

with which requests are granted or declined. This transparency would enable civil society scrutiny of corporate conduct and create accountability pressure reducing risks of complicity in human rights violations (Mann & Daly, 2019).

9.7 Creating Accessible Remedies and Redress Mechanisms

Accessible complaint mechanisms must be established enabling refugees to report concerns about biometric data processing, challenge decisions affecting them, and seek remedies for violations. These mechanisms should be available in multiple languages, should not require legal representation, and should provide timely responses addressing substantive concerns raised. Organizations implementing biometric systems should establish grievance procedures that refugees can access without fear of retaliation or assistance denial, with independent adjudication of complaints and transparent reporting of outcomes (Jacobsen, 2015).

Legal aid and advocacy support should be available to refugees seeking to challenge biometric data practices through administrative or judicial procedures. Given refugees' limited resources and legal expertise, pro bono legal services and civil society support are essential for meaningful access to justice. Data protection authorities should proactively assist refugees in exercising their rights, providing guidance navigating complaint procedures and investigating concerns even when individual refugees lack capacity to pursue formal complaints.

Compensation mechanisms should provide remedies including financial compensation, data deletion, and corrective measures when biometric data processing harms refugees. When data breaches occur exposing refugees' information, affected individuals should receive compensation reflecting the potential protection risks created by the breach, not merely nominal damages. Organizations responsible for data protection failures should bear financial responsibility for security upgrades, additional monitoring, and support services addressing harms caused by violations.

9.8 Promoting Research, Capacity Building, and Awareness

Investment in research examining the impacts of biometric identity systems on refugee populations is essential for evidence-based policy making. Research should document refugees' experiences with digital identity systems, evaluate the effectiveness of data protection safeguards, assess whether biometric systems achieve claimed benefits, and identify unintended consequences requiring mitigation. Funding should support independent researchers not affiliated with organizations implementing biometric systems, ensuring that evaluations are not compromised by conflicts of interest. Research findings should be publicly accessible and should inform policy reforms and operational improvements (Madianou, 2019).

Capacity building initiatives should strengthen data protection authorities' technical expertise and resources necessary for overseeing biometric systems. Training should cover biometric technologies' operation, privacy and security risks, auditing methodologies, and enforcement

strategies appropriate for refugee contexts. Regional networks of data protection authorities should facilitate knowledge sharing and coordinated responses to challenges that transcend national boundaries. International development assistance should prioritize supporting data protection infrastructure rather than exclusively funding biometric system deployment.

Awareness raising among refugee populations should empower individuals to understand their data protection rights and exercise agency regarding their information. Education initiatives should explain biometric technologies in accessible language, describe risks and protections, and inform refugees about complaint mechanisms and support services available. Community-based organizations working with refugees should receive training enabling them to advocate effectively on data protection issues and support refugees navigating these systems. Information campaigns should counter misinformation while honestly acknowledging both potential benefits and genuine risks associated with biometric enrollment (Livingstone, 2018).

Capacity development for government officials, humanitarian workers, and others implementing biometric systems should emphasize data protection responsibilities, ethical considerations, and protection principles that should guide digital identity governance. Training should cover consent procedures, security protocols, data sharing limitations, and appropriate responses when refugees raise concerns or encounter problems. Professional standards and codes of conduct should establish expectations for responsible biometric data handling, with accountability mechanisms addressing violations.

9.9 Developing Alternative Approaches and Exit Strategies

Policy frameworks should recognize that biometric systems are not inevitable or always appropriate for refugee contexts, and should support development of alternative approaches achieving protection and assistance objectives without requiring biometric data collection. Paper-based registration systems with adequate fraud prevention measures, anonymous assistance distribution methods, and community-based verification approaches may in some contexts better balance protection, privacy, and operational efficiency than biometric systems (Jacobsen, 2015). Cost-benefit analyses should honestly assess whether biometric systems' substantial financial investments and privacy risks are justified by marginal improvements over alternative approaches.

Exit strategies should be developed enabling transition away from biometric systems when they prove ineffective, when risks exceed benefits, or when political circumstances change rendering continued operation dangerous for refugee populations. Legal frameworks should establish data deletion requirements ensuring that biometric information is not retained indefinitely after the purposes for which it was collected have concluded. Refugees achieving durable solutions through local integration, resettlement, or voluntary repatriation should have rights to request deletion of their biometric data from systems operated by governments or humanitarian organizations unless compelling protection reasons justify continued retention.

Sunset provisions in legislation authorizing biometric systems should require periodic review and reauthorization, preventing indefinite operation without reassessment of necessity and proportionality. These reviews should include independent evaluation of whether systems have achieved stated objectives, whether privacy protections have proven adequate, and whether technological or political developments have altered risk-benefit calculations. Parliamentary oversight should ensure that biometric systems serving refugee populations remain subject to democratic accountability and can be discontinued if they fail to meet protection needs or violate fundamental rights.

10. Conclusion

The proliferation of biometric identity systems across Africa represents a profound transformation with far-reaching implications for privacy rights, human dignity, and refugee protection. This research has demonstrated that while digital identity technologies offer potential benefits including improved service delivery, enhanced fraud prevention, and facilitated access to rights and opportunities, they simultaneously create substantial risks to fundamental freedoms, particularly for vulnerable refugee populations. The legal frameworks governing biometric data protection across the continent remain inadequate relative to the technological capabilities being deployed and the protection needs of displaced populations who depend on these systems while lacking power to shape their governance.

The analysis reveals critical gaps between the rapid implementation of biometric identity systems and the development of comprehensive legal protections safeguarding privacy and data protection rights. Most African countries operate with data protection frameworks that are either non-existent, outdated relative to technological developments, or inadequately enforced despite legislative provisions. The Malabo Convention represents an ambitious regional harmonization effort, yet its limited ratification and non-entry into force leave substantial regulatory vacuums across the continent. International human rights frameworks including the International Covenant on Civil and Political Rights and the African Charter on Human and Peoples' Rights provide foundational protections, but their application to biometric systems requires interpretation and implementation that remain inconsistent across jurisdictions.

Case studies from Kenya, Uganda, South Africa, Ethiopia, Tanzania, and regional initiatives illustrate the diverse approaches to biometric identity governance and their varying implications for refugee protection. Progressive frameworks such as Uganda's inclusion of refugees in national identification systems demonstrate possibilities for using digital identity to advance integration and rights realization. However, even in contexts with relatively favorable legal frameworks, implementation challenges, security concerns, and inadequate data protection safeguards create vulnerabilities that may undermine protection objectives. Kenya's experience with litigation challenging the Huduma Namba system highlights the critical role of judicial oversight in enforcing privacy rights and requiring that biometric deployments meet constitutional and legal standards.

The multiplicity of actors involved in biometric identity governance—including host governments, UNHCR, humanitarian organizations, private technology providers, and regional bodies—creates complex accountability challenges. Divergent interests and priorities among stakeholders generate tensions between security imperatives, administrative efficiency objectives, protection principles, and privacy rights. The absence of clear protocols governing data sharing, the opacity of commercial relationships with technology providers, and the limited voice afforded to refugee populations in governance decisions compound these challenges. Meaningful reforms must address not only legal frameworks but also power dynamics and structural inequalities that marginalize refugees' interests in policy processes.

The principle of non-refoulement, fundamental to refugee protection, faces new challenges in the digital age when biometric databases create potential pathways for information to reach countries of origin or hostile actors. The confidentiality traditionally afforded to refugee status determination and protection processes may be compromised by digital systems that facilitate data sharing or surveillance. Legal frameworks must explicitly integrate data protection requirements with refugee protection obligations, recognizing that privacy rights are not merely technical concerns but are integral to protection in contexts where information disclosure can threaten refugees' safety and security.

Comparative analysis of international standards including the GDPR, UN principles on privacy and data protection, and frameworks from jurisdictions including India and Estonia reveals substantial room for improvement in African approaches to biometric data governance. Stronger requirements for privacy impact assessments, independent oversight, meaningful consent processes, purpose limitation, data minimization, and accessible remedies for violations should be incorporated into African legal frameworks. Regional cooperation mechanisms can facilitate shared learning, coordinated enforcement, and harmonized standards that protect individuals as they move across borders while preventing regulatory arbitrage.

The recommendations proposed in this paper encompass legislative reforms, policy changes, operational improvements, and structural transformations necessary to align biometric identity systems with human rights standards and refugee protection principles. Strengthening national data protection legislation, harmonizing regional frameworks, integrating data protection with refugee protection obligations, ensuring meaningful consent and participation, implementing technical safeguards, establishing corporate accountability, creating accessible remedies, and promoting research and capacity building represent interconnected elements of a comprehensive reform agenda. No single intervention will suffice; rather, sustained multi-stakeholder effort over time is necessary to transform biometric identity governance toward rights-respecting approaches.

Looking forward, the trajectory of biometric identity systems in Africa will shape the relationship between states and populations, citizens and non-citizens, protection actors and displaced communities for generations. The decisions made today about legal frameworks, governance structures, and operational practices will determine whether digital identity

serves as a tool for inclusion, empowerment, and protection or becomes an instrument of surveillance, discrimination, and control. For refugee populations who have already experienced profound violations of their rights through persecution and displacement, the imperative is clear: technological systems must be designed, implemented, and governed in ways that respect their dignity, protect their privacy, and advance their fundamental rights.

The digital identity revolution occurring across Africa presents both opportunities and risks that require careful navigation informed by human rights principles, protection obligations, and ethical commitments to vulnerable populations. Biometric systems are not neutral technologies but rather socio-technical assemblages that embody values, power relations, and choices about what kinds of societies we wish to build. Ensuring that these systems serve refugees rather than harm them requires legal frameworks that establish clear boundaries on data collection and use, governance structures that incorporate refugees' voices and interests, accountability mechanisms that provide remedies when violations occur, and a commitment to placing human dignity at the center of technological development.

The research presented in this paper demonstrates that legal challenges at the intersection of biometric identity, privacy rights, and refugee protection are neither abstract nor theoretical but have concrete implications for millions of displaced persons across Africa. Addressing these challenges effectively requires collaboration among governments, international organizations, civil society, academia, private sector actors, and most importantly, refugee communities themselves. The path forward demands not only better laws but also political will to implement protections, resources to build capacity, transparency to enable accountability, and humility to acknowledge when technological systems fail to serve their intended purposes.

As Africa continues its digital transformation, the question is not whether biometric identity systems will proliferate—that proliferation is already underway—but rather whether legal and governance frameworks will adequately protect the rights and dignity of those who are most vulnerable within these systems. For refugees whose survival, security, and futures depend significantly on identity documentation and access to protection, the answer to this question will determine whether Africa's digital identity revolution represents progress toward inclusion and rights realization or a dangerous erosion of fundamental freedoms. The legal frameworks, policy choices, and operational practices established in this critical period will shape refugee protection for decades to come, making the stakes of getting biometric identity governance right extraordinarily high.

References

- Adeyemi, O. (2021). Data protection and privacy in Nigeria: The journey so far. *Journal of Data Protection & Privacy*, 4(3), 234-248.
- African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection*. https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

- Amit, R., & Kriger, N. (2014). Making migrants 'il-legible': The policies and practices of documentation in post-apartheid South Africa. *Kronos*, 40(1), 269-290.
- Anthes, G. (2015). Estonia: A model for e-government. *Communications of the ACM*, 58(6), 18-20. https://doi.org/10.1145/2754951
- Bilak, A., & Caterina, M. (2018). *Refugee integration and digital identity: Regional responses in the Horn of Africa*. Internal Displacement Monitoring Centre.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 1-15.
- Breckenridge, K. (2014). *Biometric state: The global politics of identification and surveillance in South Africa, 1850 to the present*. Cambridge University Press.
- Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario.
- Council of Europe. (2018). *Convention 108+: Convention for the protection of individuals with regard to the processing of personal data*. Council of Europe Publishing.
- Donovan, K. P. (2015). The biometric imaginary: Bureaucratic technopolitics in post-apartheid welfare. *Journal of Southern African Studies*, 41(4), 815-833. https://doi.org/10.1080/03057070.2015.1065314
- Feldstein, S. (2019). *The global expansion of AI surveillance*. Carnegie Endowment for International Peace.
- Gates, K. (2011). *Our biometric future: Facial recognition technology and the culture of surveillance*. NYU Press.
- Gelb, A., & Metz, A. D. (2018). *Identification revolution: Can digital ID be harnessed for development?* Center for Global Development.
- Goodwin-Gill, G. S., & McAdam, J. (2021). *The refugee in international law* (4th ed.). Oxford University Press.
- Greenleaf, G. (2020). Global data privacy laws 2020: Despite COVID-19, 145 laws show data privacy is now a universal right. *Privacy Laws & Business International Report*, 167, 11-14.
- Hosein, G., & Nyst, C. (2013). *Aiding surveillance: An exploration of how development and humanitarian aid initiatives are enabling surveillance in developing countries*. Privacy International.
- Human Rights Watch. (2017). *Kenya: Ruling blocks closure of refugee camps*. https://www.hrw.org/news/2017/02/10/kenya-ruling-blocks-closure-refugee-camps

- Human Rights Watch. (2018). *Tanzania: Burundian refugees coerced to return home*. https://www.hrw.org/news/2018/09/14/tanzania-burundian-refugees-coerced-return-home
- Human Rights Watch. (2021). *Ethiopia: Eritrean refugees face abductions, attacks*. https://www.hrw.org/news/2021/09/16/ethiopia-eritrean-refugees-face-abductions-attacks
- Jacobsen, K. L. (2015). *The politics of humanitarian technology: Good intentions, unintended consequences and insecurity*. Routledge.
- Khera, R. (2019). Aadhaar failures: A tragedy of errors. *Economic and Political Weekly*, 54(14), 13-17.
- Livingstone, S. (2018). iRights: Balancing children's rights online. *Communications Law*, 23(1), 20-24.
- Madianou, M. (2019). Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises. *Social Media + Society*, 5(3), 1-13. https://doi.org/10.1177/2056305119863146
- Manby, B. (2016). *Citizenship in Africa: The law of belonging*. Hart Publishing.
- Mann, L., & Daly, A. (2019). (Big) data and the North-in-South: Australia's informational imperialism and digital colonialism. *Television & New Media*, 20(4), 379-395. https://doi.org/10.1177/1527476418806091
- Marwick, A. E., & boyd, d. (2018). Understanding privacy at the margins. *International Journal of Communication*, 12, 1157-1165.
- Mixed Migration Centre. (2021). *Quarterly mixed migration update: North Africa Q2 2021*. http://www.mixedmigration.org/resource/qmmu-north-africa-q2-2021/
- Namwaya, O. (2020). Kenya's digital identity ecosystem and data protection compliance. *International Data Privacy Law*, 10(4), 289-302.
- Nikoi, E. (2022). Digital identity and data protection in Ghana: Opportunities and challenges. *African Journal of Legal Studies*, 13(2-3), 215-238.
- *Nubian Rights Forum & Others v Attorney General & 6 Others*, Petition No. 56, 58 & 59 of 2019 (Consolidated) (High Court of Kenya 2020).
- Office of the United Nations High Commissioner for Human Rights. (2018). *The right to privacy in the digital age*. UN Doc. A/HRC/39/29.
- Omata, N. (2020). Refugee livelihoods and the private sector in Uganda: Spotlight on the Nakivale settlement. *Refugee Survey Quarterly*, 39(3), 272-297. https://doi.org/10.1093/rsq/hdaa011

- Privacy International. (2019). *The keys to data protection: A guide for policy engagement on data protection*. https://privacyinternational.org/data-protection-guide
- Roos, A. (2021). Core concepts and purpose of data protection law: Lessons from the European General Data Protection Regulation. *Potchefstroom Electronic Law Journal*, 24, 1-29. https://doi.org/10.17159/1727-3781/2021/v24i0a8046
- Ruggie, J. G. (2011). *Guiding principles on business and human rights: Implementing the United Nations "protect, respect and remedy" framework*. United Nations.
- Sharpe, M. (2018). *Mixed migration and refugee protection on the Asia-Pacific region*. Edward Elgar Publishing.
- Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.
- Supreme Court of India. (2018). *Justice K.S. Puttaswamy (Retd.) and Anr. v Union of India and Ors.*, Writ Petition (Civil) No. 494 of 2012.
- UN Women. (2018). *Gender and technology: Building an inclusive digital economy*. https://www.unwomen.org/en/digital-library/publications/2018/12/gender-and-technology
- UNHCR. (2018). *Policy on the protection of personal data of persons of concern to UNHCR*. https://www.unhcr.org/protection/operations/5b360f4d4/policy-protection-personal-data-persons-concern-unhcr.html
- UNHCR. (2022). *UNHCR global report 2022*. https://reporting.unhcr.org/globalreport2022
- UNHCR. (2023). *Global trends: Forced displacement in 2023*. https://www.unhcr.org/global-trends
- United Nations Human Rights Committee. (1988). *CCPR General Comment No. 16: Article 17 (Right to Privacy)*. UN Doc. HRI/GEN/1/Rev.9 (Vol. I).
- Unwanted Witness. (2021). *The state of surveillance in Uganda 2020*. https://unwantedwitness.org/the-state-of-surveillance-in-uganda-2020/
- Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer International Publishing. https://doi.org/10.1007/978-3-319-57959-7