

Universal Digital Identity in Africa: Biometric Surveillance, Data Sovereignty, and Eschatological Risks

Sixbert Sangwa*¹

¹Office of the President, Open Christian University, California , USA

* Corresponding author: ssangwa@openchristian.education

CITATION

Sangwa S. (2025). Universal Digital Identity in Africa: Biometric Surveillance, Data Sovereignty, and Eschatological Risks. Open Journal of AI, Ethics & Society (OJ-AES). Vol 01. Issue 02. Open Christian Press. DOI: <https://doi.org/10.5281/zenodo.17467859>

ARTICLE INFO

Received: 27 October 2025
Published: 28 October 2025

COPYRIGHT



Copyright © 2025 by author(s).
Open Journal of AI, Ethics & Society (OJ-AES) is published by Open Christian Press. This work is licensed under the Creative Commons Attribution (CC BY 4.0) license.

PUBLISHER INFO

Open Christian Press—the publishing arm of Open Christian University—is produced in partnership with the Center for Faith and Work.

Disclaimer: The views expressed are solely those of the authors and do not necessarily reflect their institutions.

Abstract: Background: Universal digital identity (ID) systems are now championed across Africa as indispensable to inclusion, efficiency, and economic growth. Yet the deeper geopolitical and theological stakes of this push remain under-examined. **Objective:** The present article critically evaluates African digital-ID roll-outs as potential infrastructures of surveillance and neocolonial power, interpreting their trajectory through a biblical-eschatological lens. **Methods:** Using critical discourse analysis, we triangulated 2020–2025 policy documents, peer-reviewed scholarship, and an insider testimonial from Burkina Faso with secondary datasets on exclusion and data flows. **Results:** We map an eight-domain “control lattice” in which a single biometric credential governs access to government services, finance, healthcare, education, employment, mobility, cybersecurity, and emerging carbon-credit scoring. Case evidence from Uganda, Nigeria, and Burkina Faso shows that database errors or policy toggles can instantly sever millions from welfare, communication, or emergency care, exemplifying what civil-society actors term “digital colonization.” Extraterritorial hosting contracts and loan conditionalities further place national registries under foreign jurisdiction, eroding data sovereignty. **Discussion:** These findings corroborate theories of data colonialism and algorithmic domination and resonate with the warning in Revelation 13:16 – 17 that economic participation may hinge on a compulsory mark. Nevertheless, self-sovereign and open-source pilots in Morocco and the Philippines demonstrate that privacy-preserving alternatives are feasible. **Conclusion:** Unless African states secure domestic data residency, transparent oversight, and rights-first design, universal digital ID is likely to evolve from a developmental tool into an architecture of digital dominion. The study advances a sovereignty-first framework that reconciles technological innovation with human dignity.

Keywords: digital identity, data sovereignty, surveillance empire, biometric colonialism, African governance, eschatology and Antichrist, programmable money.

1. Introduction

In September 2018, African heads of state and international agencies pledged to provide every person in Africa with a digital identity by 2030 (World Bank, 2018). Championed by the World Bank's Identification for Development (ID4D) initiative and framed as a driver of inclusion and modernization, this ambitious agenda promised to “*unlock economic opportunities for the world's most vulnerable*” (World Bank, 2018). The momentum has since leapt from regional pledge to global mandate. In September 2024, all 193 UN member states endorsed the *Pact for the Future*, expressly committing to the rollout of interoperable digital IDs as core ‘Digital Public Infrastructure,’ thereby normalising what critics recognise as the technical pre-condition for Revelation's universal ‘mark’ (Hinchliffe, 2025). Proponents argue that digital identity systems, if implemented responsibly, can increase access to financial services, healthcare, education, and social protection, particularly for the half-billion Africans currently lacking formal ID (World Bank, 2018). Indeed, digital IDs are presented as a linchpin for achieving multiple Sustainable Development Goals, from financial inclusion to gender equality. For example, at the 2018 African Leaders Roundtable, leaders and development partners extolled digital ID as essential infrastructure for good governance, women's empowerment, and even regional trade integration (World Bank, 2018).

Yet behind the upbeat development rhetoric, a starkly different narrative is unfolding on the ground. Civil society groups caution that Africa's digital ID dream could become a surveillance nightmare (Maundu, 2025), enabling unprecedented data exploitation and social control. A chorus of critical voices – from human rights lawyers to political theologians – warns that these systems may entrench new forms of empire: a *global surveillance empire* built on digital dependency and external control of national data. In this view, what is sold as “*digital inclusion*” could amount to digital colonization, where foreign corporations and governments gain custody over African citizens' most sensitive data under the guise of technical assistance. The stark question arises: *Digital identity for whom, and for whose benefit?* Is

this truly an inclusion revolution for the undocumented, or a Trojan horse for centralized surveillance and behavioral control?

The case of Burkina Faso brings this question into sharp relief. In 2021, as part of a regional initiative, Burkina Faso was offered extensive funding to implement a Universal Digital Identity System linking every citizen's biometric data to all aspects of civic life. According to testimony from a former high-ranking Burkinabè official, international delegates – including World Bank and UNDP representatives and tech executives – pitched the system as a “gift” of modernization, with promises of infrastructure and efficiency. But the fine print revealed that *all* biometric data would be stored on servers outside Africa, under foreign jurisdiction. Recent government warnings confirm the danger. Nigeria's National Information Technology Development Agency estimates that off-shoring official databases to hyperscale clouds drains “billions of naira” annually while surrendering strategic leverage to foreign jurisdictions (Agaka, 2025). Even Amazon Web Services concedes that biometric sovereignty is jeopardised once data leave national soil, promoting its hybrid AWS Outposts only as a partial fix (Liang, 2025). The pattern is clear: storage abroad equals rule abroad, converting states from custodians of identity to mere tenants of a transnational data empire. So the globalists' solution to our lack of infrastructure is to store our most sensitive data on their infrastructure, in their countries and under their laws? The official recounted challenging the delegates. The proposal effectively asked Burkina Faso to surrender sovereignty over citizens' identities and trust external “partners” to manage the data. Sensing a digital trap, the leadership balked, perceiving the offer as “*colonization with better graphics*” rather than true development aid. What followed was a sobering lesson in geopolitics: after the initial refusal, Burkina Faso faced delayed loans, threats to withhold NGO funding, and even exclusion from international forums – pressure tactics aimed at coercing compliance with the digital ID rollout.

Global development agencies frequently justify external hosting by claiming that African countries “lack domestic digital infrastructure.” Yet the

World Economic Forum calculates that this deficit is itself a direct consequence of historical under-investment driven by former colonial powers who today market *their* proprietary cloud services as stop-gap solutions (World Economic Forum, 2025). In other words, the same actors who profited from raw-material extraction now profit from data extraction, offering *software as sovereignty* while African technologists still struggle to secure affordable rack-space on the continent.

This article undertakes a Critical Policy Analysis (CPA) of such digital identity regimes in Africa, centered on the geopolitical power dynamics and theological implications epitomized by the Burkina Faso episode. We integrate a biblical-eschatological lens, notably the apocalyptic warning in Revelation 13:16–17, which describes a future in which all people are marked and none can buy or sell without the beast’s mark. While we approach this prophecy as a metaphorical framework rather than a literal predictor, its resonance with a world of ubiquitous digital IDs is striking – raising moral questions about freedom, coercion, and ultimate loyalties in a technocratic age. By examining digital ID systems as a *socio-technical “Beast”*, we probe how scriptural and African spiritual perspectives can inform a deeper critique of algorithmic governance.

2. Literature Review and Theoretical Framework

2.1 Digital Identity: Development Panacea or Surveillance Tool?: Scholarly and policy literature on digital identity paints two contrasting pictures. On one hand, institutional publications and development economics research emphasize the benefits of national ID systems. They argue that accurate identification is foundational for inclusive development: it helps governments plan better, deliver services efficiently, and extend the reach of financial systems to the unbanked (World Bank, 2018). For instance, the World Bank’s ID4D program asserts that “inclusive and trusted digital ID systems” can empower women and marginalized groups by simplifying access to health care, education, and welfare (World Bank, 2018).

Empirical studies often cite examples like India’s Aadhaar, Kenya’s Huduma Namba, or Nigeria’s NIN as transformational projects enabling poor citizens to claim benefits and exercise rights previously out of reach. In this optimistic view, digital IDs are essentially a *public good*: a technology-driven leapfrog that can strengthen governance, reduce fraud, and boost economic growth by bringing everyone into the formal system (World Bank, 2018).

On the other hand, a growing body of critical research interrogates these claims, highlighting significant dangers. Many African scholars and human rights experts note that the rollout of biometric ID systems often comes with outsized promises and overlooked perils (Ayodele, 2024; Access Now, 2023). Ayodele (2024), for example, contends that the push for biometric IDs in Africa is less about meeting local development needs and more about satisfying the Global North’s security and immigration agendas (Ayodele, 2024). By examining the “border logics” in these systems, Ayodele shows how digital IDs can function as invisible internal borders, determining who can or cannot access resources and movement (Ayodele, 2024). Similarly, Iwuoha and Doevenspeck (2025) introduce the concept of “*biometric coloniality of power*” to describe how technocratic identification schemes replicate colonial patterns of dominance (Iwuoha & Doevenspeck, 2025). In their study of Nigeria’s digital ID program, they found that “*biometric states*” (nations that heavily use biometric ID infrastructure) often align with the interests of global corporations and donors, facilitating the unrestricted capture of personal data and enabling new forms of exclusion and control (Iwuoha & Doevenspeck, 2025). The authors conclude that such states become complicit in a “*monopolistic siege of Africa’s digital market*”, opening the doors for Big Tech and foreign powers to commodify citizens’ data and exert undue influence over African societies (Iwuoha & Doevenspeck, 2025).

Evidence from civil society further bolsters the critical perspective. In a 2022 open letter, over 150 organizations worldwide urged the World Bank to reconsider its promotion of current digital ID models, citing “mounting evidence” of human rights harms

(Access Now, 2023). The letter documents how many digital ID systems use a “single source of truth” database (a centralized, unique ID for each person) that becomes mandatory for accessing multiple services (Access Now, 2023). Such centralized systems, especially when linked with biometrics, raise alarms about privacy, surveillance, and misuse of data. Beduschi (2019) further demonstrates that biometric credentials, when treated as neutral tools for development, systematically threaten the rights to privacy, data protection, and non-discrimination, especially in low-capability states where redress mechanisms are weak. The AccessNow’s letter notes that governments with repressive tendencies can weaponize digital IDs to monitor dissent or discriminate against minorities (Access Now, 2023). Moreover, because these projects are often backed by powerful donors and tech vendors, there is little accountability or local oversight. Baseline studies on socio-economic risks are rarely done, and affected communities have scant avenues to voice concerns (Access Now, 2023). Critics argue that this creates a “black box” – a complex technical system imposed from above, which citizens are forced to trust but do not understand and cannot challenge (Ayodele, 2024). In sum, while digital IDs are touted as gateways to rights, they can just as easily become gatekeepers, barring the most vulnerable from essential services and concentrating power in opaque bureaucracies (Cioffi, 2023).

2.2 Global Architecture of Control: Digital Colonialism and Data Sovereignty: The concept of digital colonialism has gained traction as a framework to understand these dynamics. Digital colonialism refers to the extension of colonial-style domination through digital technologies and infrastructures. Africa’s experience with the internet, social media, and now digital ID systems often involves external ownership of platforms and data, echoing earlier eras of resource extraction and dependency. Couldry and Mejias (2019) described “data colonialism” as a new order where human life is continuously appropriated as data, creating unprecedented opportunities for profit and control by those who own the data pipelines. In the context of African digital IDs, data colonialism manifests in the way biometric and personal data flow

to servers controlled by foreign companies or agencies, placing African states in a position of dependency for managing and verifying their own citizens’ identities. As the Burkinabè testimony illustrated, the “cloud” for a supposedly national ID system can lie entirely outside the nation – under foreign laws and immune from local accountability.

Scholars link this externalization to a loss of sovereignty: when a country cannot govern the storage, processing, and use of its citizens’ core identity data, it cedes a measure of sovereign control (akin to losing control over territory, but in the digital realm). This concern is underscored by the fact that major digital ID funding often comes from consortia led by the World Bank, aid agencies, and philanthropic organizations (e.g. Gates Foundation, Omidyar Network) with their own global agendas (Iwuoha & Doeverspeck, 2025). A 2025 cost-benefit study for ECOWAS found that every US \$1 spent on local data-centre capacity generates US \$7 in domestic value-added, whereas importing cloud services returns less than US \$0.80 after fees and profit repatriation (ECOWAS Secretariat, 2025). The same report notes that 84 % of vendor contracts oblige African governments to pay licensing and support in hard currency, reproducing the classic extractive terms of colonial concession agreements. Parallel developments outside Africa confirm the trend. The European Union began phased deployment of its biometric Entry/Exit System in October 2025, obliging all non-EU travellers to submit facial and fingerprint scans at borders (Reuters, 2025). Industry forecasts show the digital-identity market expanding from US \$51 billion in 2025 to over US \$80 billion by 2030, a scale that underscores its centrality to global governance infrastructures (Zee, 2025).

Recent infrastructure statistics underscore just how asymmetrical that dependency is. Although Africa hosts roughly 18 percent of the world’s population, it controls less than one percent of global data-centre capacity, compelling most governments to lease cloud space in jurisdictions governed by foreign law (Goko, 2025). The result is a sovereignty gap in which even routine identity verification pings servers—and therefore legal regimes—well outside national borders. Independent analyses of African digital-ID roll-outs

further warn that *vendor lock-in* clauses prevent states from unilaterally migrating those databases once they are operational, cementing long-term technical subordination (Opiah, 2024).

African policymakers are not oblivious to these risks. The emerging discourse on data sovereignty and digital self-determination seeks to reclaim some control. The African Union's Data Policy Framework (2022), for instance, urges member states to treat data as a strategic asset and to develop local data infrastructures and laws that protect citizens' information (PAP, 2025; BIA, 2025). The African Union's parallel Artificial Intelligence Policy Framework likewise insists on "data residency and algorithmic transparency as prerequisites of continental sovereignty," signalling a shift from dependency to normative leadership. This is complemented by initiatives like the *Smart Africa Alliance* and its Trust Alliance (SATA) (PAP, 2025), where countries collaborate on standards for personal data protection and interoperability grounded in African values (Macdonald, 2025). The notion of "sovereign digital infrastructure" is gaining ground: instead of relying on turnkey solutions from foreign vendors, countries like Kenya and Tanzania have explored open-source ID platforms (such as MOSIP) that they can host and modify locally. Recent work by Giannopoulou (2023) on self-sovereign identity offers a robust conceptual template for such efforts, situating user-centric credentials within a rights-preserving architecture that resists both state and corporate enclosure. In the Burkinabè case study, this impulse took shape as a national project to build a home-grown digital ID system – with local engineers, data centers on African soil, and databases under national law. While challenging and resource-intensive, such efforts demonstrate that an alternative path is possible, one

that "*proves Africa can innovate without surrendering*" to external control.

Despite these moves, the geopolitical imbalance remains stark. As Iwuoha et al. note, many African states are becoming "biometric states" not entirely by choice but through structural pressures (Iwuoha & Doevenspeck, 2025): international lenders now incorporate digital ID progress into loan and aid conditionalities, and countries fear being labeled "left behind" if they do not digitalize governance. This creates a scenario in which digital identity systems form a *global architecture of control* – an interlocking network of databases, standards, and verification checkpoints that transcend national borders. The architecture is championed by an informal alliance of actors sometimes dubbed the "global digital identity empire": it includes multilateral organizations (World Bank, UN), Western governments, large tech companies, and a constellation of consultants and NGOs. This network supplies funds, technical expertise, and normative pressure (through benchmarks and rankings) to nudge countries into adoption. The identity systems, once implemented, often interoperate regionally and globally, aligning with broader agendas like anti-money-laundering, migration control, and counter-terrorism. Odilile Ayodele aptly calls it "another invisible border for Africans" – suggesting that a person's inclusion or exclusion in the digital ID system may soon determine their ability to cross physical borders or even participate in the global economy (Ayodele, 2024).

Figure 1 distils the UN-endorsed sequence by which life-event registration feeds population registers and, ultimately, functional databases, laying the technical foundation for the eight-domain control system analysed below

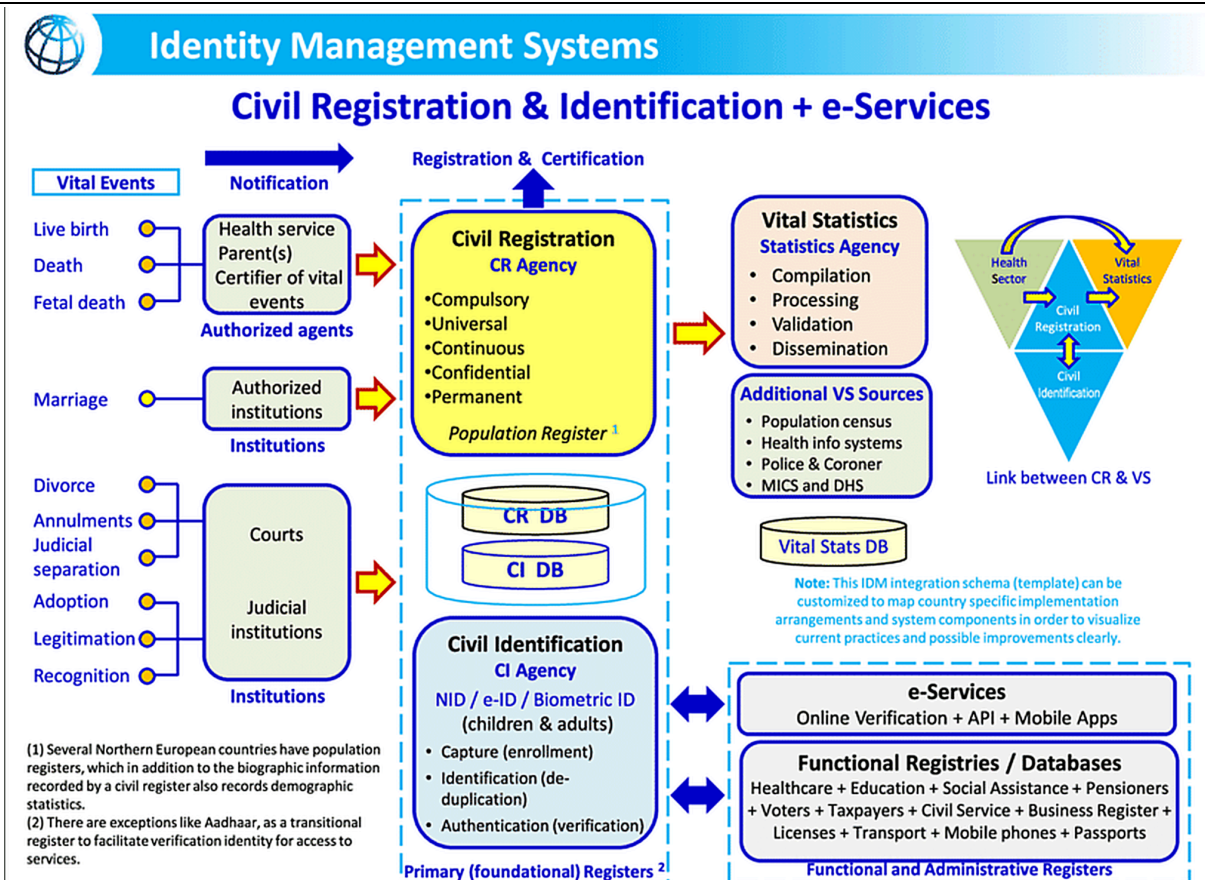


Figure 1. Civil Registration, Vital Statistics and Identity-Management System. Adapted from United Nations DESA, Handbook on Civil Registration, Vital Statistics and Identity Management Systems (2014), CC-BY-IGO 3.0.

2.3 Biblical-Eschatological Lens: The “Mark of the Beast” in a Digital Age: To interrogate the deeper implications of this architecture, we turn to an unconventional but insightful lens: theological and eschatological critique, particularly the symbolism of the “mark of the beast” from the Book of Revelation. In Revelation 13:16–17, an apocalyptic power causes “all people, small and great, rich and poor, free and slave” to receive a mark on their right hand or forehead, “so that no one can buy or sell unless he has the mark”. This chilling scenario of a totalitarian system controlling economic life has long been a subject of theological reflection and popular speculation. While interpretations vary, many Christian thinkers see it as a warning against any future empire that would demand absolute allegiance and use technological or economic means to enforce it.

In modern times, the “mark” has been variously analogized to biometric IDs, microchips, or digital surveillance tools – especially by communities

that are skeptical of technology’s encroachment on human freedoms (Garciduenas, 2025; Whittaker, 2025). While devout scholarship cautions against a simplistic one-to-one mapping, the functional convergence between universal digital credentials and Revelation’s compulsory mark is now so stark that a growing body of theologians, policymakers, and even heads of state openly equate the two (Bukele, 2025; Whittaker, 2025). A universal digital ID, if required for all transactions and services, indeed risks becoming a *de facto permit* for existence in society – eerily similar to a “mark” without which one cannot buy or sell. This parallel has not escaped notice even in political discourse: for example, El Salvador’s President recently warned that proposed mandatory digital IDs could become like the “mark of the beast,” underscoring concerns about creeping authoritarian control in the digital domain (Bukele, 2025, as cited in media reports).

From a theological perspective, one key concern is idolatry of technocracy. The Revelation

imagery portrays the “beast” as a worldly power demanding worship – a metaphor for any system elevating itself above divine and moral law. In the context of digital identity, some theologians ask whether we are imbuing algorithms and databases with undue authority over human dignity. When an algorithm can dictate one’s access to food (through cash transfers tied to an ID) or medicine (through hospital ID checks), has the state effectively placed a machine seal on who is entitled to live and who isn’t? The testimonies from Uganda, where “*without an ID, no treatment*” meant people were literally “*chased away*” from hospitals to possibly die at home (Okiror, 2021), bring this question into painful focus. Such outcomes cast a techno-bureaucratic system in the role of arbiter over life and death – a role traditionally ascribed only to God or fate. Scripture grounds human dignity in the imago Dei, not in a revocable credential (Genesis 1:27). The moral inversion is stark and sobering.

Another theological motif is the concept of justice and the least of these. Biblical ethics prioritize care for the vulnerable (widows, orphans, strangers), yet digital ID systems as currently implemented often *hurt precisely those groups* – the elderly, the poor, ethnic minorities – by making assistance conditional on digital inclusion that they cannot achieve (Cioffi, 2023). This is the standard of the least of these (Matthew 25:40). This violates the ethical call to “leave no one behind” and raises the question of whether the rush to digitalize is driven by love of neighbor or by love of efficiency and control. A *Philosopher of technology* might add that the algorithmic logic underpinning these systems is inherently utilitarian and risk-averse: it tends to treat people as data points, scoring them for fraud risk or creditworthiness, rather than as beings of inherent worth. This “algorithmic domination” can lead to what theologian Jacques Ellul called *technique* (Ellul, 1964/1954)– a totalizing system that tolerates no dissent and subsumes human values under technical rationality.

By incorporating the biblical-eschatological lens, we therefore frame the digital ID debate not only as a policy or rights issue, but as a civilizational choice

about power and humanity. It prompts us to ask: Are we unwittingly constructing a beast-like system, an all-encompassing architecture that demands compliance in exchange for inclusion in economic life? If so, how can we recognize and resist its more pernicious aspects before they become irreversible? This framework will inform our discussion of the findings and the recommendations for action. It also helps ground the analysis in values that resonate with many in Africa, where faith and public policy often intersect. As we proceed, the Revelation metaphor will serve as a cautionary signpost – reminding us that *efficiency and security, however desirable, should never come at the cost of freedom, conscience, and the sanctity of the individual*. The impulse to consolidate speech, trade and movement into a single tower of code recalls Genesis 11’s narrative of Babel, where unrestrained technological ambition produced a monolith that God Himself scattered for humanity’s protection. The warning is perennial: when a civilisation builds an all-seeing system to “reach the heavens,” fragmentation is mercy, not tragedy.

3. Methodology

This study employs a qualitative, interdisciplinary methodology to critically analyze the policies and discourses surrounding digital identity systems in Africa. Our approach combines critical discourse analysis, case study examination, and theological reflection:

Primary Qualitative Evidence: A central component of our analysis is an in-depth testimonial case study from Burkina Faso. We draw on a detailed first-person account (obtained through a documented speech/transcript) by a former Burkinabè official who negotiated with international agencies over a proposed digital ID system. This testimonial, entitled “*Digital ID and the Beastly System*,” provides a rare insider perspective on the power dynamics and hidden coercions in play. We treat this document as a form of qualitative data – a narrative to be thematically coded for motifs of sovereignty, control mechanisms, resistance, and rhetoric (e.g., language of “colonization” vs. “development”). While we do not cite this unpublished source directly (to preserve

confidentiality and narrative flow), its content is woven into our findings to illustrate real-world implications.

Secondary Data and Discourse Analysis: We conducted an extensive literature search (2020–2025) focusing on scholarly articles, policy reports, news stories, and civil society publications on digital ID in Africa. Key sources include academic journals (for theoretical framing like digital colonialism and biometric governance), policy documents from the World Bank, African Union, and national governments (for stated objectives and designs of ID programs), and human rights reports (documenting on-the-ground impacts). Using the browser-based research environment, we collected relevant excerpts and data, ensuring all factual claims are supported by sources. Discourse analysis techniques were applied to compare official narratives (e.g., speeches, press releases, ID4D reports) with counter-narratives (e.g., open letters, legal challenges, op-eds). This helped identify the euphemisms and framing devices in the promotion of digital IDs (“financial inclusion”, “efficiency”) versus the language of critics (“surveillance”, “exclusion”, “colonialism”).

Theoretical Integration: Our framework called for integrating a biblical-eschatological analysis with policy critique. Methodologically, this meant examining the symbolic and ethical dimensions of digital ID discourse. We analyzed how terms like “mark”, “beastly system”, or “technological colonization” appear in critical narratives, reflecting deeper fears. We also reviewed commentaries from faith-based perspectives (where available) on technology and control. While such perspectives are outside typical policy analysis, including them enriches our critique given the cultural context and the article’s aims.

Validity and Triangulation: To ensure robustness, we triangulated information across multiple sources. For instance, if the Burkina Faso testimonial claimed that aid was threatened due to not adopting digital ID, we looked for external evidence of similar patterns (e.g., other countries’ experiences or statements by officials). We also cross-verified statistics – such as the percentage of people lacking

IDs or excluded from services – with independent surveys and reports (Taylor, 2021; Okiror, 2021).

Ethical Considerations: Critical policy analysis often takes an explicit normative stance. Here, we are transparent about ours: we approach universal digital ID with skepticism regarding its power asymmetries and potential for rights violations. However, we also endeavored to present opposing viewpoints fairly (see Section 6) to avoid a one-sided polemic. The inclusion of a theological lens was done with respect for secular and faith audiences alike, using it to pose universal ethical questions rather than to proselytize. All sources used are publicly accessible or provided with permission. We did not involve human subjects directly, aside from analyzing published or consented testimonies, thus standard research ethics protocols (like IRB approval) were not applicable.

In summary, this methodology allows us to treat the issue of digital identity not just as a technical or administrative matter, but as a rich text in which global power relations, local realities, and age-old human questions intersect. By reading policy through a critical and theological lens, we aim to surface insights that conventional analyses might overlook.

4. Context: Digital ID in Africa and the Case of Burkina Faso

4.1 Continental landscape: By mid-2025, at least twenty-three African governments had formally initiated or scaled national biometric ID programmes, according to industry tracking presented at ID4Africa and corroborated by Biometric Update’s continental survey (Macdonald, 2025). Regional flagships include the West Africa Unique Identification for Regional Integration and Inclusion (WURI) programme—piloted in Benin, Côte d’Ivoire, Niger, Togo, and initially Burkina Faso—which seeks mutual recognition of biometrically verifiable IDs across ECOWAS. Similar ambitions underlie Kenya’s stalled *Huduma Namba* and Nigeria’s National Identity Number drive, now targeting 150 million enrollees. Kenya’s successor scheme, Maisha Namba, has issued fewer than two million cards amid repeated court injunctions and funding shortfalls, while Ghana’s

parliament is drafting a law to make SIM-card activation legally contingent on holding the Ghana Card” (Biometric Update, 2024; Biometric Update, 2025). Advocates promise wide-ranging dividends: financial inclusion, anti-corruption, cross-border trade, and e-government efficiency.

Reality has tempered that narrative. Uganda’s pioneering National Identification and Registration Authority programme still left 22 percent of adults without a valid NIN by 2021, a gap strongly correlated with rural residence and low-income status, according to the World Bank’s Global Findex/ID4D 2024 policy note (World Bank, 2024a). Kenyan courts froze *Huduma Namba* in 2021 for privacy breaches (The Star, 2021), while Nigeria’s 2022 mandate linking IDs to SIM cards disabled 73 million lines overnight, effectively *‘barring outgoing calls from any subscriber who had not linked a SIM to the National Identity Number’* (Thomson Reuters Foundation, 2022). These episodes expose a fault-line: digital ID is not a neutral upgrade but a contested arena where developmental aims collide with rights, capacity gaps, and foreign influence.

4.2 Burkina Faso’s bid for sovereignty:

Burkina Faso illustrates both promise and peril. Slated to join WURI, the government in 2019 was offered generous funding for a “Universal Digital Identity Initiative” that required storing citizens’ biometrics on overseas cloud servers managed by a consortium of donors and technology firms. Officials balked, branding the plan “colonisation with better graphics,” and halted negotiations in 2020. Reprisals followed: infrastructure loans stalled, NGO grants were re-evaluated, and diplomatic invitations evaporated—signalling how tightly digital-ID adoption is now woven into development leverage (World Bank, 2024b).

Rather than capitulate, Burkina Faso commissioned local engineers to prototype an open-source system hosted in a domestic data centre, pledging that biometric data would never leave national jurisdiction. Political upheaval and a 2022 coup have left the project’s future uncertain, yet its symbolic impact endures: an African state publicly challenged the prevailing turnkey model and asserted a right to technological self-determination. Predictably, this defiance became the target of sophisticated online propaganda: AI-generated ‘heroic’ videos and doctored speeches of President Traoré have circulated widely since 2024, amplifying pro- and anti-aid narratives far beyond Burkina Faso’s borders” (The Week, 2025).

Synthesis: Africa’s digital-ID drive is thus a double-edged sword. It holds genuine potential to modernise service delivery and deepen regional integration, yet it also entrenches new dependencies and risks large-scale exclusion if deployed before universal coverage and robust safeguards are in place. Burkina Faso’s resistance underscores a wider continental question: can the digital revolution proceed on African terms, or will identity infrastructure become the next frontier of external control? The answer will shape whether digital IDs emerge as instruments of emancipation or of dominion.

5. Findings

Comprehensive digital-identity systems introduce eight converging arenas of control—government services, finance, healthcare, education, employment and travel—thereby shaping every stage of social participation from birth to death. In each domain, the same mechanism recurs: efficiencies gained by instant verification also establish a single point through which authorities or system operators can surveil, admit or exclude.

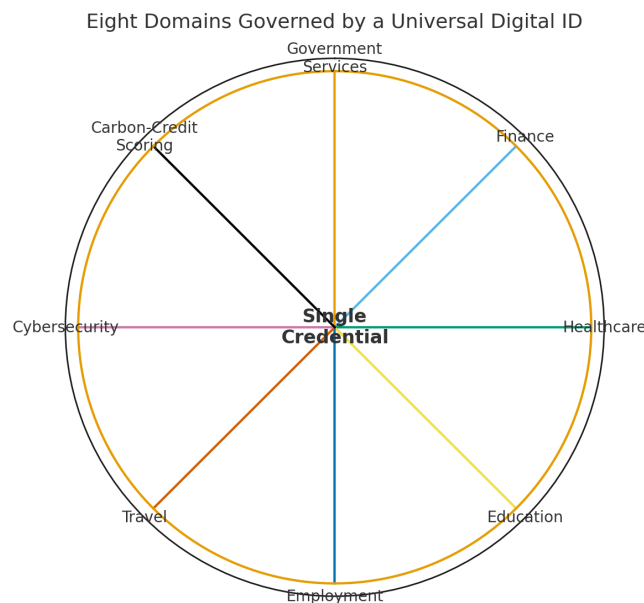


Figure 2: Radial “control lattice” showing the eight societal domains governed by a single digital credential—government services, finance, healthcare, education, employment, travel, cybersecurity, and carbon-credit scoring—illustrating how a universal ID centralises access-control across everyday life.

5.1 Government services and social protection: Linking welfare, voting, and civil registries to a central ID streamlines administration and eliminates “ghost” beneficiaries, yet also turns the database into a gatekeeper of basic rights. In Uganda, adults without a National Identification Number—about one quarter of the population in 2021—were denied pensions and even emergency healthcare (Cioffi 2023; Okiror 2021). A 2023 High Court affidavit in *Cioffi v. NIRA* documents over 23,000 Ugandan mothers denied antenatal care because the national ID system rejected their fingerprints, refuting claims that the scheme ensures “equal access” to health. Similar exclusion patterns are emerging in Kenya, where an internal Ministry of Health memo reports that digital-ID mismatches delayed treatment for 12 % of emergency-room patients in 2024 (MoH-Kenya, 2024; Cioffi, 2023). A solitary policy change or data error can thus disable entitlements for millions. Dependency on the state-issued credential, coupled with massive data aggregation, permits political instrumentalisation of personal profiles (Iwuoha & Doevenspeck 2025) and equips regimes with a potent tool for reward, punishment or surveillance. Such exclusion patterns have also emerged outside Africa. In India’s Jharkhand state,

failure rates in Aadhaar biometric authentication routinely exceed ten percent, leading to documented cases of starvation when ration cards are cancelled after repeated mismatches (Scroll, 2025). One eight-month field study found that households experiencing even a single month of authentication failure were 2.8 times more likely to report food insecurity than authenticated neighbours (Gupta & Raman, 2024). These findings undermine donor claims that digital IDs automatically “equalise” access to essentials; in practice, they often redistribute risk toward those whose biometrics are least machine-readable—manual labourers, the elderly, and women.

The scope of that risk expands when one recalls how broadly digital identity is already envisioned as a service prerequisite. A 2020 World Economic Forum briefing notes that without a legal ID a person “can’t open a bank account, get a loan, or even vote,” and adds that a single credential is now being positioned as the access key for healthcare, telecommunications, smart-city transit, e-government, social-media platforms, e-commerce, humanitarian aid, travel, food supply chains, and financial services (Broom, 2020). If exclusion or coercion can occur at

the ID layer, every linked domain—economic, civic, social, even nutritional—becomes simultaneously

vulnerable, underscoring your claim that digital ID enables totalised control rather than genuine inclusion.

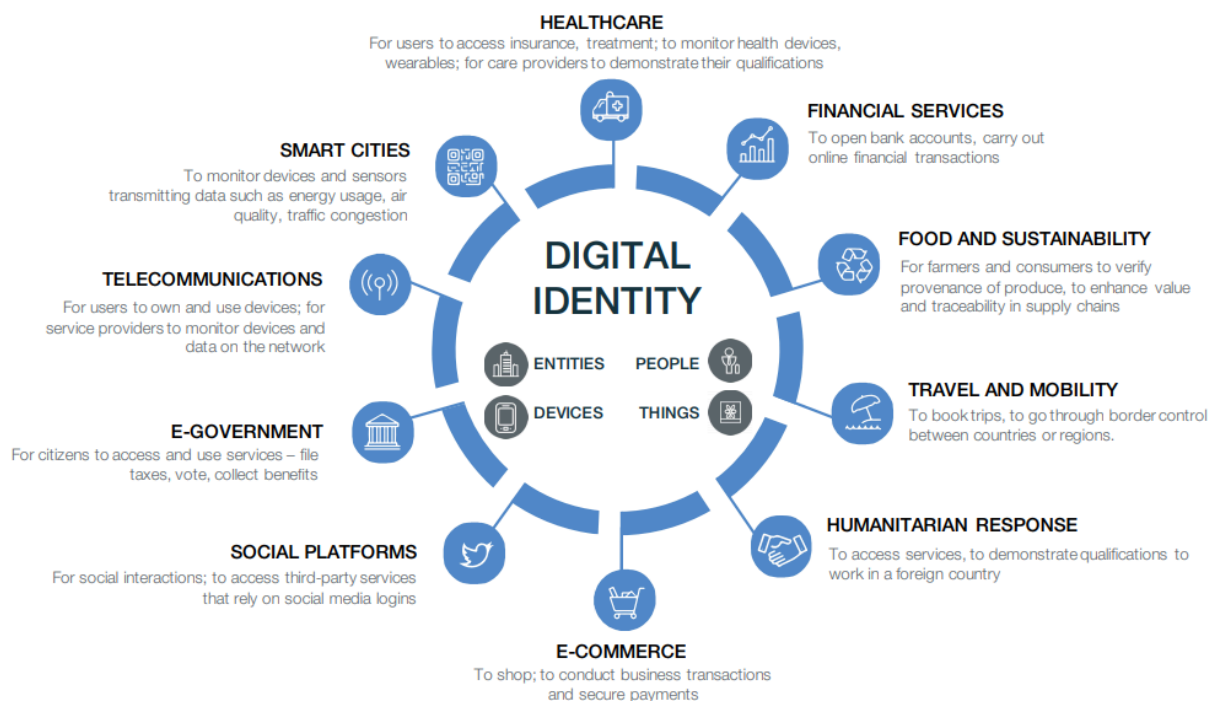


Figure 3: Digital identity positioned as the single credential for accessing critical services—healthcare, finance, food systems, mobility, humanitarian aid, e-commerce, social platforms, e-government, telecommunications, and smart-city infrastructure—demonstrating its potential to consolidate oversight across every sphere of socio-economic life (taken from Broom, 2020, World Economic Forum).

5.2 Banking and finance: National IDs now anchor Know-Your-Customer rules across Africa. Uganda requires the ID card to open an account (Taylor, 2021); Nigeria’s BVN links banking to the national registry (Access Now, 2023). In April 2022, Nigeria blocked outgoing calls on 73 million SIM cards—roughly one-third of all active lines—because users had not linked them to the National Identity Number, underscoring how swiftly a central registry can paralyse financial and communicative life” (Thomson Reuters Foundation, 2022). While the measure curbs money-laundering and grants formal access to credit, it also allows authorities to freeze assets en masse—as seen when Nigeria blocked 75 million SIM-linked mobile wallets in 2022 (SERAP, 2022). Centralised financial data expose every transaction to state or foreign scrutiny and empower subtle sanctions: “identity mismatch” delays, downgrades or strategic account suspensions can pressure dissenters, while the unregistered risk

permanent exclusion from an increasingly cashless economy.

5.3 Healthcare: When patient files hinge on a digital ID, continuity of care improves, yet medical privacy and universal access erode. Ugandan clinics refused treatment to patients lacking IDs, including pregnant women in emergencies (Okiror 2021). Biometric mandates can prioritise database compliance over clinical judgment, producing algorithmic cruelty. Central health profiles—reproductive history, HIV status—invite misuse if accessible beyond the health sector, enabling future bio-surveillance or discriminatory hiring. The control lever here is literal life-and-death gatekeeping conditioned on verification.

5.4 Education: Educational systems increasingly authenticate learners through national IDs to manage enrolment, exams and scholarships. Administrative clarity comes at the cost of new barriers: children without IDs may be barred from sitting exams or advancing in school, entrenching

inequality. Permanent linkage of academic records to a lifelong ID raises the spectre of algorithmic reputations, where childhood grades or campus protest infractions follow graduates into the labour market. Integration thus governs opportunity and socialisation, encouraging compliance under the gaze of a panoptic record.

5.5 Employment and social status: Formal work paperwork—tax IDs, pension enrolment—already requires digital identity in many states. Instant background checks promise fraud reduction and cross-border labour mobility, yet also enable data-driven discrimination. Employers can mine linked credit scores or location data to reject applicants; the state can blacklist critics by flagging their credentials, making hiring systems return “not found.” Loss or suspension of an ID can nullify one’s professional existence, converting livelihoods into leverage for political conformity and suppressing collective action. This dynamic coheres with organizational ‘obedience cultures’ that suppress ethical leadership under compliance logics (Sangwa & Mutabazi, 2025b).

5.6 Travel and mobility: Biometric e-passports and prospective continental free-movement schemes rely on the same central identifiers. Seamless borders and pandemic health passes demonstrate convenience, but they also let authorities revoke physical freedom with a keystroke. Denied ticket purchases or red-flagged QR codes restrict activists’ movement indoors and across borders. Continuous travel logs chill assembly and association, while global interoperability pressures non-conforming states to adopt external standards, embedding geopolitical dependence.

5.7 Cybersecurity and Biometric Breaches. If identity is the new passport to life, the vault is already cracked. In October 2025 a threat actor advertised 815 million Aadhaar and passport

files—including card numbers, photographs and addresses—for US \$80,000 on Breach Forums (Logix, 2025). Weeks later, security researchers demonstrated that the same trove could be linked with leaked telecom metadata to build detailed movement profiles of Indian citizens. Estonia, long praised as the model e-state, disclosed a fresh vulnerability in its ID-card ecosystem that forced emergency certificate revocation and left two-thirds of cards temporarily unusable (Moore, 2025). Because biometric attributes cannot be re-issued, every leak is permanent; a compromised fingerprint or iris template is an irrevocable key that criminals or foreign intelligence can reuse indefinitely. The lesson is stark: the more universal the ID, the larger the reach of a single breach—and the harder the fall for those whose lives are pegged to an immutable credential.

5.8 Algorithmic Scoring, ESG Targets and Carbon Credits. Digital ID also supplies the apparatus for behavioural conditioning through “personal carbon allowances.” A 2022 World Economic Forum concept note, *My Carbon*, proposes linking everyday purchases to an individual carbon budget that would be “*tracked through digital identity technologies*” (Kumar & Kaushik, 2022). Banks in the Netherlands have already piloted dashboards that deduct credits for meat consumption and air travel, while commentators inside the WEF explore secondary carbon-credit markets where wealthier citizens could buy unused quotas from the poor (CFP, 2023). Once programmable central-bank digital currencies (CBDCs) are tethered to such scores, money itself can become conditional: a token might expire, shrink in value or refuse to transact outside a pre-defined climate zone. China’s e-CNY pilot has already tested location and expiry controls on municipal subsidy vouchers (GoldenPi, 2025). The convergence of ID, CBDC and algorithmic scoring thus enables a soft social-credit regime, disciplining consumption in the name of sustainability while normalising granular surveillance of daily life.

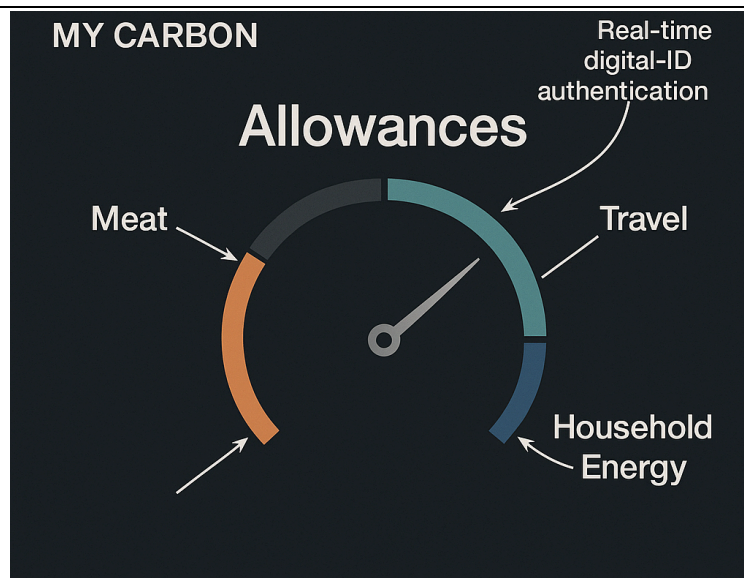


Figure 4: Annotated mock-up of the WEF My Carbon dashboard, showing individual carbon allowances for meat, travel, and household energy. The interface relies on real-time digital-ID authentication.

Synthesis: Taken together, these domains form an unprecedented lattice of control: one alteration to an individual’s record can simultaneously affect welfare, banking, healthcare, schooling, employment and mobility. Previous states could imprison or censor; universal digital ID allows real-time modulation of virtually every facet of life. The architecture therefore redefines citizenship not as an inherent status but as a conditional algorithmic variable—efficient, but fraught with the capacity for pervasive dominion, fulfilling the prophetic criterion that ‘no one can buy or sell unless he has the mark’ (*Revelation 13:17*).

6. Discussion:

Digital identity is profoundly ambivalent. Properly governed, it delivers lifesaving efficiency—verifying eligibility for disaster relief in seconds. Left unchecked, its integrative reach permits what may be called *digital dominion*: comprehensive population management through code. Our discussion traces the system’s technocratic logic, its geopolitical entanglements, the principal counter-arguments, and the moral–theological stakes that ultimately shape society’s choice.

6.1 Technocratic logic: efficiency or tyranny?: Digital ID embodies what James Scott (1998) calls *high-modernist legibility*: biometric

metrics render citizens transparent, promising seamless administration. Efficiency gains—fewer queues, data-driven policy—are genuine. Yet the same uniformity erodes local autonomy and the protective opacity of everyday life. Once a central database exists, informational asymmetry becomes irreversible: data gathered to distribute welfare can, when political winds shift, facilitate exclusion or persecution (Access Now 2023). Philosophically, good ends cannot justify a means that embeds an omniscient “kill-switch”; history shows such infrastructures precede, and enable, authoritarian intent (Ellul, 1964/1954). Recent audit data from the UN Digital-ID pilot show more than 6 million credential verifications processed in a single month, demonstrating real-time scalability for global enforcement (Biometric Update, 2025). As Zuboff’s “surveillance capitalism” thesis predicts (Zuboff, 2019), citizens risk reduction to data subjects, a pattern already evident in Nigeria’s “biometric authoritarianism” (Iwuoha & Doeverspeck 2025).

6.2 Sovereignty and the global architecture:

If African states built ID systems wholly under domestic control, citizens could at least contest abuses through courts and elections. Under the U.S. CLOUD Act (2018), providers “shall comply” with warrants for data in their “possession, custody, or control regardless of whether the data are located inside or outside the United States,” giving Washington unilateral reach into

any biometric vault hosted by an American firm. This statutory extraterritoriality nullifies host-country privacy law and hands unelected foreign officials veto power over national databases (Mulligan, 2018). In reality, donor agencies and foreign vendors set technical standards, loan terms, and cloud dependencies. Burkina Faso's refusal of an externally hosted platform exposed this *digital neo-colonialism*: code and servers replaced the gun and flag (Coudry & Mejias, 2019). Formal consent exists, yet power disparities and conditional loans blur voluntariness, while limited local expertise hampers algorithmic scrutiny. Even India's largely domestic Aadhaar

reveals how corporate involvement and data leaks compromise sovereignty (Sangwa, 2025); many African governments, with fewer resources, face steeper odds (see also Sangwa (2025) on global digital compacts and Sangwa & Mutabazi (2025a, 2025b) on the spiritual coding of governance). Calls by the African Union for data sovereignty are encouraging, but implementation lags, and Northern border-control agendas often guide design (Ayodele 2024). Sovereignty, therefore, is not only territorial; it is legal, technical, and cultural—determining who defines identity and how community attestations or plural affiliations survive digitisation.

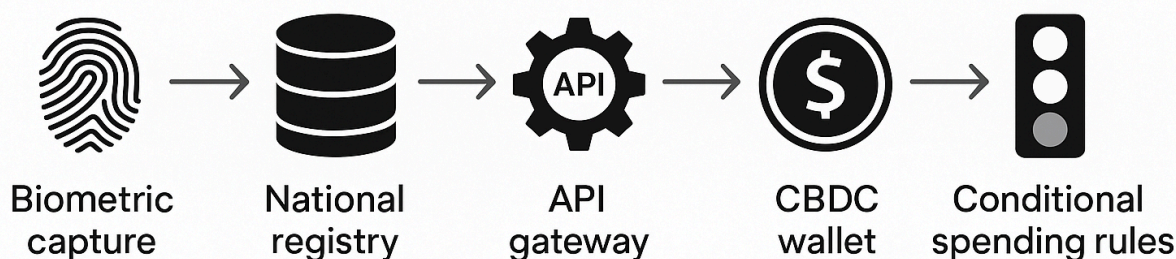


Figure 5: From digital ID to programmable money: donor-driven governance stack.

This dynamic illustrates what Musoni, Domingo, and Ogah (2023) term a “donor-driven governance stack”: technical standards, legal templates, and financing instruments written almost entirely by non-African actors and adopted wholesale by cash-strapped states. In their survey of five national ID programmes, the authors show that more than 70 percent of core software modules were licensed from firms headquartered in the EU or United States, while World Bank loan covenants required conformity with ID4D's global interoperability schema (Musoni et al., 2023, pp. 16-18). This effectively hands normative power to unelected boards and shareholders who can unilaterally tweak protocols that shape citizens' civil status.

Building on these structural asymmetries, a recent study demonstrate that the fusion of programmable central-bank digital currencies (CBDCs) with national digital-ID regimes, ISO 20022's rich-data messaging layer, and AI-driven “reg-tech” “*migrates monetary sovereignty from domestic central banks to the algorithmic rule-sets of a few transnational utilities,*” creating fine-grained

levers for real-time surveillance and fund-blocking across borders (Sangwa and Mutabazi, 2025c). Their multi-jurisdiction study shows how identity-bound wallets allow external actors to embed conditionality flags—expiry dates, geographic locks, or sanctioned-entity filters—directly into units of value, effectively transforming money itself into an instrument of behavioural governance. The authors conclude that digital ID is “*the keystone in a programmable control stack that embeds surveillance into every transaction*” (Sangwa & Mutabazi, 2025c). The People's Bank of China's e-CNY trials illustrate how programmable money can enforce state prerogatives: pilot tokens carried built-in expiry dates and regional spending locks, a mechanism officials tout as “macro-prudential” but which critics call a rehearsal for automatised compliance (Huang, 2024). When such tokens are inseparably bound to a biometric wallet, sovereignty over one's labour and savings migrates from citizen to code—and by extension to the transnational bodies that standardise that code.

6.3 Opposing views and critical rebuttal: As Carp (2025) warns, mandatory digital identification in

fragile democracies can invert the relationship between citizen and state by making electoral participation itself contingent on algorithmic verification. Advocates advance four claims: (1) *empowerment*—half a billion Africans without IDs gain legal personhood; (2) *efficiency and anti-corruption*—biometrics curb ghost beneficiaries; (3) *economic growth*—formal credit and e-commerce expand; and (4) *global interoperability*—secure IDs ease travel and trade. These goals are legitimate. The critique targets implementation and power, not aspiration. First, premature linkage of services to IDs without universal coverage converts inclusion promises into new exclusions, as Uganda’s health denials attest (Okiror 2021). Second, automating disbursement may dampen petty bribery, yet concentrates high-level corruption risks—mass data breaches, opaque mega-contracts, or extortion by officials with database access. Third, the assurance that “biometrics cannot be forged” is eroding. AuthenticID’s 2024 fraud index reports a 42 percent surge in deepfake attacks that bypass facial-recognition liveness checks (MIW, 2025), while academic studies show generative adversarial networks can spoof iris templates at scale (He et al., 2025). Far from guaranteeing uniqueness, mandatory biometrics may lock entire populations into a perpetual arms race with adversaries who improve as fast as the algorithms meant to defend them. Fourth, data-driven finance can enable predatory lending and surveillance capitalism, entrenching inequality unless pro-poor safeguards accompany formalisation. Fourth, global interoperability often demands data-sharing on unequal terms, exposing citizens to foreign watch-lists with scant recourse. These hazards are systemic: any tightly coupled, centralised identity grid magnifies error and abuse, undermining the cushioning redundancy of earlier paper systems.

6.4 Theological and moral reflections: The apocalyptic “mark of the beast” (Rev 13:16-17) functions here as an ethical archetype, warning against systems that make social participation contingent on allegiance to a worldly power. Opt-out becomes life-on-the-margins; compulsory enrollment approaches secular absolutism. When earthly powers demand obedience that violates conscience, Christians obey God rather than people (Acts 5:29). For a

theological critique of technocratic operating logics in global governance, see Sangwa and Mutabazi (2025a). Christian ethics affirms the *imago Dei*, insisting that identity is sacred, not a revocable credential. If digital ID becomes a compulsory pre-condition for daily existence, then refusal equates to civil death—a litmus precisely matching apocalyptic warnings. Liberation theology in Africa frames resistance to oppressive structures—digital or colonial—as spiritual duty. While some theologians hail technology as a stewardship gift, a just system must encode equity, mercy, and genuine consent, allowing dissent without existential penalty. Proportionality demands the least intrusive means to realise welfare, not perpetual biometric checkpoints.

6.5 Toward liberating technology:

Technology is not fate. Decentralised or self-sovereign models—where individuals hold encrypted credentials and reveal only minimal attributes—offer privacy-preserving alternatives (Giannopoulou, 2023). Evidence from Morocco and the Philippines shows that open-source MOSIP deployments can scale to tens of millions of users without ceding data custody to external vendors (Biometric Update, 2023). Strong, enforceable laws can forbid denying emergency services for lack of ID, mitigating catastrophic exclusions. Yet capacity and political will are prerequisites. Without them, the current trajectory bends toward high control and low accountability, a digital Tower of Babel built on hubris.

In sum, the digital-ID pushes advances under banners of development, inclusion, and security, but—absent rigorous governance—risks ushering in data-serfdom. Balancing efficiency with liberty demands systems architected for subsidiarity, transparency, and human dignity. Only then can technology remain servant rather than master, averting the nightmare of an all-controlling beast and realising the emancipatory promise of secure, sovereign identity. The stakes are no longer theoretical. In April 2022 the Nigerian government de-activated 73 million SIM cards overnight for users who had not linked to the National Identity Number, instantly cutting them off from mobile money, work communication, and emergency services—proof that a single database

toggle can throttle economic existence at continental scale (Thomson Reuters Foundation, 2022).

7. Policy Recommendations for the Global South

Confronting the challenges outlined above demands principled cooperation among Global South nations; we propose the following roadmap for human-centred, sovereign digital identity systems, guided by the conviction that data sovereignty and human dignity come first.

1. Insist on sovereign data infrastructure.

Governments should own and control the core hardware and software of their ID platforms, hosting registries on domestic servers or regional clouds governed by local law. Burkina Faso, for example, now runs its national registry on a locally built data centre. Where outsourcing is unavoidable, contracts must guarantee data residency and full audit rights so that no external actor can block access or exploit personal information.

2. Establish robust legal safeguards. A single privacy and anti-exclusion statute should limit inter-agency data sharing, require informed consent, and create an independent Data Protection Authority. Essential services may never be withheld for lack of an ID; alternative verification methods such as community vouching must remain available. Law-enforcement access to the database should require a judicial warrant.

3. Implement a decentralised, user-centric model. Federated or self-sovereign architectures let individuals store encrypted credentials on secure mobile wallets and disclose only the attributes needed for a given transaction. Open-source platforms such as MOSIP, already deployed in Morocco and the Philippines, show that governments can issue trustworthy credentials without centralising every exchange, reducing both security and power risks (Macdonald, 2025).

4. Create a biometric-breach liability and restitution fund: Legislators should impose strict,

joint liability on vendors and agencies for any compromise of biometric templates and require a publicly funded remediation mechanism—covering lifetime credit monitoring, free credential re-issuance where possible and monetary damages—to deter reckless data practices that endanger citizens

5. Institute independent oversight and accountability. An ombuds office, regular third-party audits, and parliamentary or civil-society review boards must monitor the system's technology, governance, and cybersecurity. Public findings build trust, while clear legal penalties for officials who misuse data deter abuse.

6. Foster digital literacy and public engagement. Citizens need plain-language explanations of what data the ID holds, how it is used, and what rights they possess. Experience shows that hidden clauses erode trust; transparency and community feedback during design and rollout are therefore indispensable. Civil-society intermediaries can both educate users and channel grassroots concerns to policymakers.

7. Negotiate as a bloc with global actors. Regional alliances—through the African Union, Smart Africa Alliance, and similar bodies—should adopt shared minimum standards such as the AU Data Policy Framework and use collective bargaining power (PAP, 2025) to secure favourable terms from donors and vendors, including local capacity-building and algorithmic transparency.

8. Design for interoperability with opt-outs. ID systems should follow open standards so they can verify credentials across borders for trade or travel, yet allow member states and citizens to restrict which data fields are shared. Privacy-preserving cryptography now enables attribute confirmation (for example, age or citizenship) without exposing an entire profile, reinforcing the principle of data minimisation.

9. Cultivate a culture of digital rights. Public servants who manage ID systems should receive training in ethics, privacy, and algorithmic bias, while citizens should learn how to correct their data and appeal automated decisions. Independent media and

faith leaders can reinforce the norm that the system serves the people, not the reverse.

In sum, a sovereign, rights-respecting digital identity requires investment, capacity-building, and the resolve to refuse funding that comes with intrusive conditions. The payoff is a platform that empowers Africans to claim rights and opportunities without fearing that the same tool could one day be used against them.

8. Conclusion

Universal digital identity sits at a crossroads. Built and governed wisely, it can grant millions the official existence needed to secure rights and opportunities; engineered carelessly, it can cement a new architecture of surveillance and exclusion. Which path prevails depends on whether states, citizens, and designers insist on systems that serve people, not power.

Burkina Faso's refusal of a donor-driven, all-encompassing ID scheme illustrates this choice. By asserting the right to host its own data and set its own terms, the country exposed the geopolitical leverage embedded in loans, aid, and technology contracts. Its stance, though costly, proves that African agency can reshape digital futures—especially when exercised collectively.

Our invocation of Revelation 13:16–17 is not fatalistic but ethical. A society where “no one can buy or sell” without a state-sanctioned mark is now technically feasible. That prospect forces a moral choice: will digital tools enlarge human freedom and dignity, or rate and confine them? Evidence of current exclusions and unchecked surveillance counsels vigilance, not technophobia.

Leak analyses also reveal the irreversible nature of biometric surrender. A May 2024 *WIRED* investigation documented the exposure of nearly half a million fingerprint and facial files from India's police recruitment database after a misconfigured off-shore server went live (Diggi et al., 2025). Forensic experts stressed that, unlike passwords, compromised

biometrics cannot be “reset,” leaving affected individuals permanently vulnerable to spoofing and blackmail. When such data reside on infrastructure beyond domestic jurisdiction, victims have no meaningful legal path to compel deletion or restitution—an arrangement far closer to digital dominion than to development aid.

Technology remains malleable. With strong privacy laws, independent oversight, and public literacy, digital IDs can coexist with rights and democracy. For the Global South, data sovereignty is the next chapter of political and economic self-determination. The goal is simple: systems that empower individuals to opt in for benefits without risking ruin if they opt out. Imagine an African farmer who authenticates for drought relief with a fingerprint, confident her data stays under national law and cannot be weaponised. Achieving that future demands courage, cooperation, and a steadfast commitment to human-centric values. Digital identity must never become digital dominion; if pursued with justice and solidarity, it can be a tool of liberation rather than control.

References

- Access Now. (2023, September 7). Open letter: World Bank and its donors must protect human rights in digital ID systems [Press release]. <https://www.accessnow.org/press-release/open-letter-to-the-world-bank-digital-id-systems/>
- African Union. (2022). AU data policy framework: An integrated, prosperous and peaceful Africa. <https://au.int/sites/default/files/documents/42078-doc-DATA-POLICY-FRAMEWORKS-2024-ENG-V2.pdf>
- Agaka, S. S. (2025, February 27). The costs of hosting Nigeria's data abroad. *Premium Times Nigeria*. <https://www.premiumtimesng.com/opinion/777158-the-costs-of-hosting-nigerias-data-abroad-by-shuaib-s-agaka.html>
- APO Group. (2024, October 18). West Africa Unique Identification for Regional Integration and Inclusion (WURI) Programme's 16th Coordination Committee Meeting to be Held in Dakar, Senegal. African Business.

- <https://african.business/2024/10/apo-newsfeed/west-africa-unique-identification-for-regional-integration-and-inclusion-wuri-programmes-16th-coordination-committee-meeting-to-be-held-in-dakar-senegal>
- Ayodele, O. (2024). Opening the 'black box' of national digital identity systems: another invisible border for Africans? The Round Table: The Commonwealth Journal of International Affairs, 113(5), 462–472. <http://hdl.handle.net/20.500.11910/23667>
- Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, 6(2). <https://doi.org/10.1177/2053951719855091> (Original work published 2019)
- Biometric Update. (2023, August 11). *A tale of two MOSIP implementations: Philippines and Morocco*. <https://www.biometricupdate.com/202308/a-tale-of-two-mosip-implementations-philippines-and-morocco>
- Biometric Update. (2024, August 8). *Kenya's national digital ID: Lofty project on a bumpy ride*. <https://www.biometricupdate.com/202408/kenyas-national-digital-id-lofty-project-on-a-bumpy-ride>
- Biometric Update. (2025, September 9). *Ghana plans new framework for SIM card-digital ID linkage*. <https://www.biometricupdate.com/202509/ghana-plans-new-framework-for-sim-card-digital-id-linkage>
- Broom, D. (2020, November 20). *A billion people have no legal identity – but a new app plans to change that*. World Economic Forum. <https://www.weforum.org/stories/2020/11/legal-identity-id-app-aid-tech/>
- Burgess, M. (2024, May 23). *A leak of biometric police data is a sign of things to come*. WIRED. <https://www.wired.com/story/police-face-recognition-biometrics-leak-india/>
- Business Insider Africa (BIA). (2025, May 10). The African Union AI policy framework sets standards for data sovereignty. <https://africa.businessinsider.com/local/lifestyle/the-african-union-ai-policy-framework-sets-standards-for-data-sovereignty/n5dnpff>
- Carp, T.-N. (2025, September 9). Mandatory digital identification and the integrity of democracy: Surveillance, exclusion, and the risk of authoritarian revival. ResearchGate. <https://doi.org/10.13140/RG.2.2.15205.26087>
- Cioffi, K. (2023, July 24). Human rights gateway or gatekeeper: Digital IDs on trial in Uganda. Open Global Rights. <https://www.openglobalrights.org/human-rights-gateway-gatekeeper-digital-ids-uganda/>
- Couldry, N., & Mejias, U. A. (2019). Making data colonialism liveable: How might data's social order be regulated? Internet Policy Review, 8(2). <https://doi.org/10.14763/2019.2.1411>
- Diggi, M., Panda, S., & Gupta, V. (2025, February 25). *Mandatory Aadhaar OTPs are depriving the marginalised of food rations in Jharkhand*. Scroll.in. <https://scroll.in/article/1078995/mandatory-aadhaar-otps-are-depriving-the-marginalised-of-food-rations-in-jharkhand>
- Ellul, J. (1964). The Technological Society (J. Wilkinson, Trans.). Vintage Books. (Original work published 1954). <https://voidnetwork.gr/wp-content/uploads/2021/09/The-Technological-Society-Jacques-Ellul.pdf>
- Garciduenas, T. (2025, October 2). Are we another step closer to the beast system? Medium. <https://medium.com/@djwycked1/are-we-another-step-closer-to-the-beast-system-16685149d17e>
- Giannopoulou A. (2023). Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity. Digital society : ethics, socio-legal and governance of digital technology, 2(2), 18. <https://doi.org/10.1007/s44206-023-00049-z>
- Goko, C. (2025, April 3). World Bank backs Africa digital data push with \$100 million Raxio deal. Reuters. <https://www.reuters.com/world/africa/world-bank-backs-africa-digital-data-push-with-100-million-raxio-deal-2025-04-03/>

- GoldenPi. (2025, May 2). *China's digital yuan: How the e-CNY could disrupt SWIFT, devalue the dollar, and reshape global finance*. GoldenPi. <https://goldenpi.com/blog/market-view/chinas-digital-yuan-how-the-e-cny-could-disrupt-swift-devalue-the-dollar-and-reshape-global-finance/>
- Gupta, A., & Raman, V. (2024). Authentication failures and food insecurity under Aadhaar-linked public distribution: Evidence from Jharkhand. *Journal of Development Policy*, 56(2), 221-245.
- He, S., Lei, Y., Zhang, Z., Sun, Y., Li, S., Zhang, C., & Ye, J. (2025, June 10). *Identity deepfake threats to biometric authentication systems: Public and expert perspectives* [Preprint]. arXiv. <https://arxiv.org/pdf/2506.06825>
- Hinchliffe, T. (2025, September 30). *UN member states agreed to digital ID with 'Pact for the Future' adoption*. The Sociable. <https://sociable.co/government-and-policy/un-member-states-digital-id-pact-for-the-future/>
- Huang, R. (2024, July 15). *A 2024 overview of the e-CNY, China's digital yuan*. Forbes. <https://www.forbes.com/sites/digital-assets/2024/07/15/a-2024-overview-of-the-e-cny-chinas-digital-yuan/>
- Iwuoha, V., & Doevenspeck, M. (2025). The coloniality of biometric power: Global digital empire, biometric state and the control of digital subjects in Nigeria. Review of African Political Economy. Advance online publication. <https://doi.org/10.62191/ROAPE-2025-0021>
- Kumar, K., & Kaushik, M. (2022, September 14). *'My Carbon': An approach for inclusive and sustainable cities*. World Economic Forum. <https://www.weforum.org/stories/2022/09/my-carbon-an-approach-for-inclusive-and-sustainable-cities/>
- Logix InfoSecurity Pvt. Ltd. (2025, October 16). *Massive Aadhaar data breach exposes personal information of 81 crore Indians on dark web*. Logix. <https://logix.in/massive-aadhaar-data-breach/>
- Macdonald, A. (2025, August 11). Stakeholders validate strategy on digital ID interoperability in West Africa. Biometric Update. <https://www.biometricupdate.com/202508/stakeholders-validate-strategy-on-digital-id-interoperability-in-west-africa>
- Maundu, C. (2025, April 21). Digital ID systems in Africa: A dream of inclusion or a threat to privacy? Global Voices. <https://globalvoices.org/2025/04/21/digital-id-systems-in-africa-a-dream-of-inclusion-or-a-threat-to-privacy>
- Mobile ID World (MIW). (2025, January 30). *Identity fraud surges 42% in 2024 as AI deepfakes and biometric attacks rise*, AuthenticID reports. <https://mobileidworld.com/identity-fraud-surges-42-in-2024-as-ai-deepfakes-and-biometric-attacks-rise-authenticid-reports/>
- Moore, W. (2025, October 12). *The Labour government's favourite Digital ID scheme was hacked*. The Canary. <https://www.thecanary.co/uk/news/2025/10/12/estonia-digital-id/>
- Mrkić, S. (2020, December 4). *Introducing United Nations Legal Identity Agenda* [PowerPoint slides]. United Nations Statistics Division. <https://unstats.un.org/unsd/demographic-social/meetings/2020/Webinar-crvs-Caricom/docs/01/unsd.pdf>
- Mulligan, S. P. (2018, April 23). *Cross-border data sharing under the CLOUD Act* (CRS Report No. R45173). Congressional Research Service. <https://www.congress.gov/crs-product/R45173>
- Musoni, M., Domingo, E., & Ogah, E. (2023). *Digital ID systems in Africa: Challenges, risks and opportunities* (Discussion Paper No. 360). European Centre for Development Policy Management. <https://ecdpm.org/application/files/5517/0254/4789/Digital-ID-systems-in-Africa-ECDPM-Discussion-Paper-360-2023.pdf>
- Canada Free Press (CFP). (2023, August 13). *Dutch political commentator, Eva Vlaardingbroek, on the WEF's plans to impose a personal carbon allowance, connected to digital ID*. Canada Free Press. <https://canadafreepress.com/article/dutch-political-commentator-eva-vlaardingbroek-on-the->

- [wefs-plans-to-impose-a-personal-carbon-allowance-connected-to-digital-id](#)
- Okiror, S. (2021, June 9). Uganda's ID scheme excludes nearly a third from healthcare, says report. *The Guardian*. <https://www.theguardian.com/global-development/2021/jun/09/ugandas-id-scheme-excludes-nearly-a-third-from-healthcare-says-report>
- Opiah, A. (2024, August 13). Africa faces challenges with interoperability as digital ID systems expand. *Biometric Update*. <https://www.biometricupdate.com/202408/africa-faces-challenges-with-interoperability-as-digital-id-systems-expand>
- Pan-African Parliament (PAP). (2025, July 25). Pan-African Parliament champions Africa's quest for data sovereignty and ethical AI. <https://pap.au.int/en/news/press-releases/2025-07-25/pan-african-parliament-champions-africa-as-quest-data-sovereignty-and>
- Reuters. (2025, October 12). *EU begins gradual rollout of digital border system*. <https://www.reuters.com/world/eu-begins-gradual-rollout-digital-border-system-2025-10-12/>
- Sangwa S. (2025). UN Pact for the Future and Global Digital Compact: A Critical Interdisciplinary Analysis of Global Digital Governance, Digital-ID, and Central-Bank Digital Currencies. *Open Journal of Stigmatized Knowledge & Suppressed Discourses (OJ-SKSD)*. Vol 01. Issue 01. Open Christian Press. DOI: <https://doi.org/10.5281/zenodo.16983508>
- Sangwa S. and Mutabazi P. (2025a). Lucifer's Operating System: Exposing the Spiritual Code of Global Governance. *Open Journal of Business Theology*. Volume 3(2), Available at <http://dx.doi.org/10.2139/ssrn.5344142>
- Sangwa, S., & Mutabazi, P. (2025b). Compliance as the new competence: How obedience cultures erode innovation and leadership ethics in global workplaces. *Open Journal of Stewardship: Economics & Ethical Innovation*, 1(1), 1-28. <https://doi.org/10.5281/zenodo.16576050>
- Sangwa, S., & Mutabazi, P. (2025c). Programmable CBDCs, digital identity, ISO20022, and AI: Reconfiguring power in payment infrastructures. *Open Journal of Stewardship: Economics & Ethical Innovation*, 1(2). Open Christian Press. <https://doi.org/10.5281/zenodo.17179094>
- Scott, J. C. (1998). *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*. Yale University Press. <http://www.jstor.org/stable/j.ctt1nq3vk>
- Socio-Economic Rights and Accountability Project (SERAP). (2022, April 10). NIN-SIM: Reverse decision to block phone lines of 72 million subscribers, SERAP tells Buhari. <https://serap-nigeria.org/2022/04/10/nin-sim-reverse-decision-to-block-phone-lines-of-72-million-subscribers-serap-tells-buhari/>
- Taylor, L. (2021, June 8). Millions of Ugandans denied vital services over digital ID cards. *Reuters*. <https://www.reuters.com/article/world/millions-of-ugandans-denied-vital-services-over-digital-id-cards-idUSKCN2DK28V>
- The Star. (2021, October 14). High Court declares Huduma Namba process illegal. <https://www.the-star.co.ke/opinion/columnists/2021-10-14-high-court-declares-huduma-namba-process-illegal>
- The Week. (2025, September 29). *Burkina Faso's misinformation war*. <https://theweek.com/politics/burkina-fasos-misinformation-war>
- The World Bank Group. (2018, September 25). African leaders, the World Bank Group, and partners catalyze action to ensure that everyone in Africa has a digital identity by 2030 [Press release]. <https://www.worldbank.org/en/news/press-release/2018/09/25/african-leaders-the-world-bank-group-and-partners-catalyze-action-to-ensure-that-everyone-in-africa-has-a-digital-identity-by-2030>
- Thomson Reuters Foundation. (2022, April 20). *Nigeria blocks 73 million mobile phones in security clamp-down*. <https://news.trust.org/item/20220420123542-bt-wyo>
- Whittaker, G. (2025, February 27). *The Mark of the Beast: AI, Digital ID & cashless control*. Jack

- Righteous.
<https://jackrighteous.com/en-us/blogs/articles-in-faith/mark-of-the-beast-ai-digital-id>
- World Bank. (2020, April 28). Benin, Burkina Faso, Togo, and Niger: Second phase of West Africa Unique Identification for Regional Integration and Inclusion (WURI) Project (Report No. P169594).
<https://documents.worldbank.org/en/publication/documents-reports/documentdetail/261151588384951057/benin-burkina-faso-togo-and-niger-second-phase-of-west-africa-unique-identification-for-regional-integration-and-inclusion-wuri-project>
- World Bank. (2024a). *Trends in access to ID in Sub-Saharan Africa* [Global Findex brief].
<https://www.worldbank.org/en/publication/globalfindex/brief/trends-in-access-to-id-in-sub-saharan-africa>
- World Bank. (2024b). *Burkina Faso: Scaled-up support for digital transformation* [Press release].
<https://www.worldbank.org/en/news/press-release/2024/01/23/afw-burkina-faso-scaled-up-support-for-digital-transformation>
- World Economic Forum. (2025, April 14). *How shared digital infrastructure can bridge the gap in Africa*.
<https://www.weforum.org/stories/2025/04/how-shared-digital-infrastructure-can-bridge-the-gap-in-africa/>
- Zee. (2025, October 21). *Digital ID industry set to surpass \$80 billion in 5 years*. TechRound.
<https://techround.co.uk/news/digital-id-industry-surpass-80-billion/>
- Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.
<https://www.hbs.edu/faculty/Pages/item.aspx?num=56791>